

明細書

BEST AVAILABLE COPY

視聴制御装置、視聴制御プログラム、セキュアモジュール

技術分野

5 本発明は、放送されたコンテンツや蓄積されたコンテンツの視聴を制御する視聴制御装置、視聴制御プログラム、セキュアモジュール、コンテンツを記録した記憶媒体等に関し、特に、広告の視聴を条件にコンテンツの視聴を可能にしたものである。

10 背景技術

従来から、デジタルコンテンツは、放送や、DVDなどの記憶媒体に記録されてユーザに提供され、コンテンツに対する対価は、ユーザが記憶媒体の購入費や放送の視聴料の形で支払ったり、コンテンツに付して放送した広告の広告主から徴収したり、または、コンテンツの視聴時に課金する方式(pay per view: P P V)等が取られている。

15 コンテンツの対価をユーザが支払う有料放送では、コンテンツが暗号化鍵(スクランブル鍵) K_s で暗号化(スクランブル)されて放送され、それと共に、スクランブル鍵 K_s や番組の視聴条件に関する情報を含む番組情報(E CM : Entitlement Control Message)がワーク鍵 K_w で暗号化されて放送される。

20 このスクランブル鍵 K_s は数秒ごとに更新される。

一方、視聴契約を結んだユーザの受信装置は、E CMを復号するためのワーク鍵 K_w や、契約条件の情報を含む個別情報(E MM : Entitlement Management Message)を放送から受信し、このEMMが、受信装置に装着されたI Cカードで保持される。

25 放送されたコンテンツをユーザが視聴する場合は、受信装置で受信したE CMが K_w で復号化され、EMMの契約条件が、E CMに含まれる番組の視聴条件を満たしているか否かが判定され、視聴条件を満たしているとき、また、P

PVでは、さらに番組購入の処理が行われたとき、ECMに含まれるK_sがK_wで復号化され、このK_sを用いて、受信したコンテンツのデスクランブルが行われる。

また、コンテンツを記憶媒体に記録して提供する場合は、著作権を守るために5コンテンツを暗号化して記憶媒体に記録し、コンテンツの購入者に記憶媒体とコンテンツの復号鍵とを提供する方式が考案されている。

一方、放送するコンテンツの対価を広告主から徴収する場合は、コンテンツが、広告と共にスクランブル無しに放送される。これを受信した視聴者は、広告を視聴する見返りとして、コンテンツを無料で視聴することができる。

しかし、近年、放送で提供されるコンテンツは、一度、蓄積装置に貯えられてから視聴されるようになり、そのため、コンテンツに広告を付して放送しても、再生時には、広告を飛ばして、コンテンツだけを再生視聴する場合が増えている。こうした状況は、放送媒体を利用する広告の効果を減殺させることになる。

特許文献1（特開2002-157516号公報）には、放送されて蓄積された広告の視聴を促進するように考案された広告情報提供方法が提案されている。この方法は、ユーザが広告を視聴することによって、放送受信端末を安価にレンタルできるようにするものであり、放送されて蓄積された広告をユーザが再生視聴すると、その履歴がハードディスクに記録されて広告発行サイトへ

通知され、広告の再生視聴時間に応じて次の月のレンタル料金が割り引かれる。

しかし、放送したコンテンツの対価を広告の広告主から徴収する方式は、広告主にとって広告がユーザに広く知れ渡ると言うメリットがあり、また、ユーザにとってコンテンツが無料で視聴できると言う利点がある。しかし、放送されたコンテンツを一旦蓄積して好きなときに再生する近年の視聴形態は、前述するように、広告をスキップしてコンテンツだけを再生することが可能になるため、放送を利用する広告の効果を失わせ、広告主の放送離れを招き、広告料をベースとしたコンテンツの提供を困難にする虞がある。

また、蓄積された広告の視聴を促す方策を講じたとしても、過去に放送して蓄積された、鮮度の落ちた広告が視聴されるのでは、広告主の希望を満足させることはできない。

一方、コンテンツが蓄積または視聴された時に課金する方法は、個々の視聴者から料金を徴収しなければならないため、料金の回収コストが掛かるという問題がある。また、コンテンツの視聴前に課金されるので、内容を確かめないままコンテンツを購入することに躊躇する傾向があり、それほどの収入が得られないという問題がある。また、この課金方法は、企業の宣伝広告の場を奪うことにもなる。

10

発明の開示

本発明は、こうした従来の問題点を解決するものであり、広告の視聴を条件にコンテンツの視聴を可能にする視聴制御装置、視聴制御プログラム、セキュアモジュールを提供し、また、そのコンテンツを記録した記録媒体等を提供することを目的としている。

前記目的を達成するため、本発明の一形態では、コンテンツの識別情報と当該コンテンツの視聴有効期限を示す視聴条件情報を処理モジュールで保持し、前記視聴条件情報を更新する視聴条件更新情報に対応付けられた広告を再生した場合、前記視聴条件更新情報に基づいて、前記処理モジュールで保持している前記視聴条件情報を更新部により更新し、前記視聴条件情報に基づき前記コンテンツの再生制御がするように視聴制御装置を構成している。なお、この明細書では、コンテンツの視聴制御に関する各種装置、デバイス、セキュアモジュール、時刻補正サイト、広告発行サイトを個々に、または、それらの組み合わせを視聴制御装置と呼ぶこととする。

また、本発明の他の形態では、コンピュータを、コンテンツの識別情報と当該コンテンツの視聴有効期限を示す視聴条件情報を保持し、前記視聴条件情報を更新する視聴条件更新情報に対応付けられた広告を再生した場合、前記視聴

条件更新情報に基づいて、保持している前記視聴条件情報を更新し、前記視聴条件情報に基づき前記コンテンツの再生制御するよう機能させるように視聴制御プログラムを構成している。

また、本発明の他の形態では、視聴対象の暗号化済コンテンツとその暗号化済コンテンツの視聴可能な有効期限とを指定するコンテンツの視聴条件情報を保持し、前記視聴条件情報で指定された有効期限に基づき前記暗号化済コンテンツを復号化して再生させるセキュアモジュールであって、前記視聴条件情報で指定された前記暗号化済コンテンツの有効期限を更新する視聴条件更新情報が対応付けられた広告が再生された場合、前記視聴条件更新情報に基づいて前記視聴条件情報を更新し、前記視聴条件更新情報で指定された前記暗号化済コンテンツの視聴を可能にするようにセキュアモジュールを構成している。

図面の簡単な説明

図1は、本発明の第1の実施形態における視聴制御装置の構成例を示す図、
15 図2は、広告の構成の一例を示す図、
図3は、EMM更新要求情報の構成の一例を示す図、
図4は、視聴者が広告を視聴する前のEMMの構成の一例を示す図、
図5は、視聴制御装置の広告再生動作の一例を示すフローチャート、
図6は、視聴者が広告を視聴した後のEMMの構成の一例を示す図、
20 図7は、視聴制御装置の暗号化コンテンツ再生動作の一例を示すフローチャート、
図8は、本発明の第2の実施形態における視聴制御装置の構成例を示す図、
図9は、本発明の第2の実施形態の視聴制御装置の動作を示すフローチャート、
25 図10は、本発明の第3の実施形態における視聴制御装置の構成例を示す図、
図11は、本発明の第3の実施形態の視聴制御装置の動作を示すフローチャート、

図 1 2 は、本発明の第 4 の実施形態における視聴制御装置の構成例を示す図、
図 1 3 は、本発明の第 4 の実施形態の視聴制御装置の動作を示すフローチャート、

図 1 4 は、本発明の第 5 の実施形態における視聴制御装置の構成例を示す図、
5 図 1 5 は、本発明の第 6 の実施形態における視聴制御装置の構成例を示す図、
図 1 6 は、本発明の第 7 の実施形態における視聴制御装置の構成例を示す図、
図 1 7 は、本発明の第 8 の実施形態における視聴制御装置の構成例を示す図、
図 1 8 は、本発明の第 9 の実施形態における視聴制御装置の構成例を示す図、
図 1 9 は、本発明の第 1 0 の実施形態における視聴制御装置の構成例を示す
10 図、

図 2 0 は、本発明の第 1 1 の実施形態における視聴制御装置の構成例を示す
図、

図 2 1 は、本発明の第 1 2 の実施形態における視聴制御装置の構成例を示す
図、

15 図 2 2 は、本発明の第 1 3 の実施形態における視聴制御装置の構成例を示す
図、

図 2 3 は、本発明の第 1 4 の実施形態における視聴制御装置の構成例を示す
図、

20 図 2 4 は、本発明の第 1 5 の実施形態における視聴制御装置の構成例を示す
図、

図 2 5 は、本発明の第 1 6 の実施形態における視聴制御装置の構成例を示す
図、

図 2 6 は、本発明の第 1 7 の実施形態における視聴制御装置の構成例を示す
図、及び、

25 図 2 7 は、本発明の第 1 8 の実施形態における視聴制御装置の構成例を示す
図である。

発明を実施するための最良の形態

以下、本発明の実施の形態について、図面を用いて説明する。なお、本発明は、これら実施の形態に何等限定されるものではなく、その要旨を逸脱しない範囲で種々の態様により実施することができる。

5 (第1の実施形態)

本発明の第1の実施形態では、広告が視聴されたときにコンテンツの視聴を可能にする視聴制御装置の基本構成について説明する。

この装置は、図1のブロック図に示すように、広告1011、スクランブルされた暗号化済コンテンツ1012及び鍵Kwで暗号化されたECM1013を出力する
10 再生／放送装置101と、保持している鍵Kw1022を用いてECM1013から鍵
Ks103を取り出すセキュアモジュール102と、暗号化済コンテンツ1012を
鍵Ks103で復号化して暗号解除コンテンツ105を出力するデスクランプ
104と、広告1011及び暗号解除コンテンツ105を表示する表示装置106とを
備えている。
15 再生／放送装置101は、広告1011、暗号化済コンテンツ1012及びECM1013
を生成し、無線や有線回線で放送・送信する放送装置であり、あるいは、この
放送装置から受信した広告1011、暗号化済コンテンツ1012及びECM1013
を蓄積して再生・出力する再生装置である。この広告1011には、対象のコン
テンツとそのコンテンツの視聴が可能な有効期限とを指定するEMM更新要求
20 10111が含まれており、このEMM更新要求10111は鍵Kw1022で暗号化さ
れている。また、ECM1013には、コンテンツをデスクランブルするための鍵
Ks103と視聴可能条件を示す情報とが含まれており、それらは鍵Kw1022で
暗号化されている。

セキュアモジュール102は、受信装置に装着または組み込まれており、デス
25 クランプ104は受信装置の一部を構成している。このセキュアモジュール
102には、コンテンツの視聴条件を示すEMM1021と、EMM更新要求10111
及びECM1013を復号化するための鍵Kw1022とが保持されている。このE

MM1021 及び鍵Kw1022 は、従来のシステムと同様に、予め放送されてセキュアモジュール 102 に格納される。

セキュアモジュール 102 は、また、EMM更新要求 10111 を受けたときに、それを鍵Kw1022 で復号化し、EMM更新要求 10111 の情報（即ち、EMM
5 更新要求 10111 で指定されたコンテンツと、そのコンテンツの視聴可能な有効期限の情報）をEMM1021 に設定するEMM更新部 1024 と、ECM1013 を
鍵Kw1022 で復号化して、その中に記載されているコンテンツを識別し、EM
M1021 に設定されているそのコンテンツの視聴可能な有効期限と現在時刻と
を比較して、視聴可能な場合にECM1013 から鍵Ks103 を抽出するKs 抽出
10 部 1023 とを備えている。

このセキュアモジュール 102 は、いわゆるCASカード（限定受信を目的としたカード）やICカードであり、外からのデータの不正な読み出しや書き込みが不可能で、不整なアクセスをしようとするとき破壊される媒体で作成されている。

15 なお、EMM更新要求 10111 では、コンテンツの視聴可能な有効期限として、広告の放送時刻または蓄積時刻からの一定時間を指定する。有効期限の終了時刻を具体的に指定しても良い。また、現在時刻から一定時間有効期限としても良い。

この視聴制御装置の動作について説明する。まず、再生／放送装置 101 は、
20 EMM更新要求 10111 を含む広告 1011 と暗号化済コンテンツ 1012 とを再生または放送する。広告 1011 と暗号化済コンテンツ 1012 との再生または放送は同時である必要はない。暗号化済コンテンツ 1012 を再生または放送する時には、それと同期したECM1013 を再生または放送する。再生または放送された広告 1011 は表示装置 106 で表示されるものとする。

25 セキュアモジュール 102 内のEMM1021 は、最初はどのコンテンツも視聴不可能と設定されている。セキュアモジュール 102 のEMM更新部 1024 は、表示された広告 1011 に含まれるEMM更新要求 10111 を受信すると、鍵Kw

1022 で復号化して、EMM更新要求 10111 で指定されたコンテンツとそのコンテンツの視聴可能な有効期限とを EMM1021 に設定する。

次に、K_s抽出部 1023 は、ECM1013 を受信すると、ECM1013 を鍵K_w1022 で復号化して、その中に記載されているコンテンツを識別し、EMM 5 1021 に設定されているそのコンテンツの視聴可能な有効期限と現在時刻とを比較して、視聴可能な場合に ECM1013 から鍵K_s103 を抽出してセキュアモジュール 102 から送出する。

デスクランプ 104 は、暗号化済コンテンツ 1012 と鍵K_s103 とを受信して、暗号化済コンテンツ 1012 を鍵K_s103 で復号化し、暗号解除コンテンツ 10 105 を送出する。この暗号解除コンテンツ 105 は表示装置 106 で表示される。

この視聴制御装置の視聴制御により、コンテンツの視聴は、そのコンテンツのEMM更新要求 10111 を含む広告 1011 を視聴し、且つ、そのコンテンツの視聴時点が、EMM更新要求 10111 で規定された有効期限内である場合にのみ可能になる。

15 コンテンツに対するEMM更新要求 10111 は、そのコンテンツと共に放送する広告 1011 に含めるだけでなく、その後に放送する広告 1011 にも含めることができる。この場合、視聴者は、最近放送または蓄積された広告を見るにより、以前に蓄積されたコンテンツの視聴条件が満たされ、このコンテンツの再生視聴が可能になる。

20 次に、広告が視聴されたときに暗号化済コンテンツの視聴を可能にする視聴制御装置の詳細動作について説明する。

視聴制御装置は、鍵K_s103 で暗号化された暗号化済コンテンツ 1012、広告 1011、ECM1013 を復号する鍵K_w1022、ECM1013 を再生／放送装置 101 に蓄積している。暗号化済コンテンツ 1012、広告 1011、鍵K_w1022、ECM 25 1013 は、ネットワーク、または放送または、SDカード、DVDなどの記録メディア経由により取得してもよく、取得方法に関しては本発明では特に限定しない。

図2は、広告1011の構造の一例を示す図である。

広告1011は、広告本体1901と、EMM更新要求情報10111とから構成される。EMM更新要求情報10111は、第三者に容易に書き換えられないように鍵Kw1022で暗号化されている。

5 図3は、EMM更新要求情報10111の構造の一例を示す図である。

EMM更新要求情報10111は、契約情報を保持しており、契約情報として暗号化済コンテンツを識別するコンテンツID2001と、コンテンツID2001の視聴可能な有効期限を表す情報2002から構成される。有効期限とは、コンテンツIDで表される暗号化済コンテンツの視聴許可の開始時刻を示す開始時間10 2003と、視聴許可の期限を相対的に表す継続期間2004で構成される。開始時間2003と継続期間2004とは、広告スポンサーの意図に基くものであるため、センターであらかじめ設定される。EMM更新要求情報10111の内容は、現在のデジタル放送などで用いられているEMMと内容は同じである。なお、図3に示すEMM更新要求情報10111の場合、コンテンツID2001が「100」のコンテナで、開始時間2003が「2000.01/01」、継続期間2004が「3日間」であること示している。

次に、ECM1013の内容について説明する。ECM1013の内容は、現在のデジタル放送などで用いられているECMと内容は同じであり、暗号化済コンテンツを識別するコンテンツID2001と、そのコンテンツを暗号化した鍵Ks 20 103から構成される。

次に、EMM1021の内容について説明する。EMM1021の内容は、現在のデジタル放送などで用いられているEMMと内容は同じであり、契約情報リストから構成され、契約情報は、復号可能な暗号化済コンテンツを識別するコンテンツID2001と、暗号化済コンテンツの復号可能な有効期限から構成され 25 る。

以下、視聴者が広告を視聴する場合の視聴制御装置の広告再生動作と、視聴者が暗号化済コンテンツを視聴する場合の視聴制御装置の暗号化コンテンツ再

生動作について説明する。

図4は、視聴者が広告を視聴する前のEMM1021の構成の一例を示す図である。

広告視聴前では、視聴制御装置は、コンテンツID2301が「200」の暗号化済みコンテンツ1012については2000年1月1日から1日間、コンテンツID2301が「300」の暗号化済みコンテンツ1012については、2000年1月2日から1日間、視聴可能となっているが、それ以外の暗号化済コンテンツ1012は視聴可能とはなっていない。

このような状況下で視聴者が2000年1月1日に広告を視聴する場合の視聴制御装置の広告再生動作について、図5のフローチャートを参照して説明する。

再生／放送装置101は、広告1011を表示装置106に渡す。これにより広告1011が再生され、視聴者は広告を視聴する（ステップ2101）。

次に再生／放送装置101は、広告1011に含まれるEMM更新要求情報10111をセキュアモジュール102に渡す（ステップ2102）。セキュアモジュール102のEMM更新部1024は、鍵Kw1022でEMM更新要求情報10111を復号する（ステップ2103）。

EMM更新部1024は、EMM更新要求情報10111の契約情報、本例では、図3に示すコンテンツID2001が「100」、開始時間2003が「2000年1月1日」、継続期間2004が「3日間」でEMM1021の契約情報を書き込む（ステップ2104）。

図6は、視聴者が広告を視聴した後のEMM1021の状態を示す図である。

EMM更新部1024がEMM更新要求情報1011に基づき更新したEMM1021により、広告視聴後では、視聴制御装置は、図4に示すように、コンテンツID2301が「200」、「300」の暗号化済みコンテンツ1012に加え、コンテンツID2301が「100」の暗号化済みコンテンツ1012が2000年1月1日から3日間、視聴可能となる。

次に視聴者が広告を視聴した翌日の2000年1月2日にコンテンツID2301

が「100」の暗号化済コンテンツを視聴する場合の視聴制御装置の暗号化コンテンツ再生動作について、図7のフローチャートを用いて説明する。

再生／放送装置 101 は、コンテンツ ID2301 が「100」の暗号化済コンテンツ 1012 をデスクランプ 104 に渡す（ステップ 2201）。

5 再生／放送装置 101 は、ECM1013 をセキュアモジュール 102 のKs抽出部 1023 に渡す（ステップ 2202）。Ks抽出部 1023 は、ECM1013 を鍵Kw 1022 で復号し、ECM1013 に記述されているコンテンツ ID2301 を取得する。本例ではコンテンツ ID2301 が「100」を取得する（ステップ 2203）。

10 Ks抽出部 1023 は、EMM1021 にこのコンテンツ ID2301 が「100」に関する契約情報が設定されているかどうかをチェックする（ステップ 2204）。契約情報がない場合は暗号化コンテンツの復号を中止する（ステップ 2205）。

15 ここで、契約情報がある場合、図6に示すようなEMM1021 から契約情報として有効期限 2302 を取得する（ステップ 2206）。現在時刻が有効期限 2302 の開始時間 2303 から（開始時間 2303+継続期間 2304）の間にあるかどうかをチェックする（ステップ 2207）。

現在時刻が開始時間 2003 と、（開始時間 2303+継続期間 2304）との間にない場合は、コンテンツ ID2301 が「100」の暗号化済コンテンツ 1012 の復号を中止する（ステップ 2208）。

20 本例では、現在時刻が 2000 年 1 月 2 日、開始時間 2303 が 2000 年 1 月 1 日、（開始時間 2003+継続期間 2004）は 2000 年 1 月 4 日となり、現在時刻はこれらの中に存在するので、このまま処理を続ける。現在時刻が開始時間 2303 と、（開始時間 2303+継続期間 2304）との間にある場合、Ks抽出部 1023 は ECM1013 から鍵Ks 103 を取り出し、デスクランプ 104 に送出する（ステップ 2209）。デスクランプ 104 は鍵Ks 103 を取得すると、暗号化済コンテンツ 1012 を鍵Ks 103 で復号し、表示装置 106 に渡す（ステップ 2210）。

なお、実実施形態では、デジタル放送のCAS技術（ECM、EMM）を利用した例を示したが、本発明はデジタル放送のCAS応用に限定されるもので

はなく、契約情報を伝送する仕組と、それを受信装置内部で管理する仕組（EMMに相当）と、鍵情報を伝送する仕組とそれを受信装置内部で管理する仕組（ECMに相当）を持つコンテンツ配信システム全般に適用可能である。

また、本実施形態では、セキュアモジュールを利用する例を示したが、これ
5 はEMM情報、鍵Kwなどの改竄を防止するためのものであり、別の仕組でこれら視聴制御に関する情報の改竄防止を実現してもよく、セキュアモジュールを構成の必須条件としているものではない。

また、本実施形態では、EMM等の視聴条件の保持、更新を行う処理モジュ
10 ルとしてセキュアモジュール102を利用する例を示したが、ノンセキュアな処理モジュールであってもよい。

また、本実施形態では、広告及びコンテンツが映像である場合を想定して説明したが、広告及びコンテンツは、音声その他のデータが混在しているものや音声のみのものでもよい。また、その場合、表示装置は、それぞれの形式の広告やコンテンツを表現できるものであれば良い。

15 なお、広告視聴開始時刻から広告視聴終了時刻のうちの任意の時点または広告取得時刻を基準時刻としてコンテンツの視聴有効期限を算出してもよい。

このように、この視聴制御装置では、コンテンツの視聴に先立ち、蓄積保存された古い広告ではなく、その視聴時に有効な広告を見せることができる。そのため、広告主は、商品等の新しい広告を効果的に見せるための手段を得ることができる、視聴者は、広告を見ることでコンテンツを無料で視聴できる。また、
20 コンテンツ提供者は、過去に放送したコンテンツを対象として広告収入を得ることができる。

(第2の実施形態)

本発明の第2の実施形態では、広告の最初から最後まで視聴されたときにコンテナの視聴を可能にする視聴制御装置について説明する。
25

この装置では、図8に示すように、再生／放送装置201から送出される広告2011の最後に、鍵Kw2022で暗号化された後にさらに鍵Kw2(2025)で暗

号化されたEMM更新要求2(20111)が含まれ、また、広告2011の最初に、鍵Kw2(2025)を鍵Kw2022で暗号化したKw2情報20112が含まれている。EMM更新要求2(20111)の情報内容は、第1の実施形態のEMM更新要求10111と同じであり、対象のコンテンツと、そのコンテンツの視聴可能な有効期限とが記述されている。

一方、セキュアモジュール202は、Kw2情報20112を鍵Kw2022で復号化して鍵Kw2(2025)を抽出するKw2抽出部2024と、EMM更新要求2(20111)を鍵Kw2(2025)で復号化し、その情報をさらに鍵Kw2022で復号化して、得られたEMM更新要求2(20111)の情報をEMM2021に設定するEMM更新部2023とを備えている。その他の構成は第1の実施形態(図1)と変わりがない(図8では、表示装置106やデスクランプ104等の図示の一部を省略している)。

この視聴制御装置の動作について、図9を参照して説明する。

まず、再生／放送装置201は、EMM更新要求2(20111)とKw2情報20112とを含む広告2011を再生または放送し、広告2011が表示装置106にて表示される(ステップ3101)。Kw2情報20112は広告の最初に再生または放送され(ステップ3102)、Kw2抽出部2024は、Kw2情報20112を受信すると、Kw2情報20112を鍵Kw2022で復号化して(ステップ3103)、鍵Kw2(2025)を抽出する(ステップ3104)。

次に、EMM更新要求2(20111)が広告の最後に再生または放送され(ステップ3105)、EMM更新部2023は、EMM更新要求2(20111)を受信すると(ステップ3106)、これを鍵Kw2(2025)で復号化し(ステップ3107)、その情報を鍵Kw2022で復号化して、EMM更新要求2(20111)で指定されたコンテンツを有効期限まで視聴可能とする情報をEMM2021に設定する(ステップ3108)。

その後は、第1の実施形態と同様に、EMM2021に設定されている情報を基にコンテンツの表示を制御する。

このように、この視聴制御装置では、広告の先頭と最後とを視聴しないとコンテンツを見ることが出来ないので、広告を確実に視聴させることができる。

(第3の実施形態)

本発明の第3の実施形態では、広告が先頭から最後まで早送りをせずに視聴
5 されたときにコンテンツの視聴を可能にする視聴制御装置について説明する。

この装置では、図10に示すように、EMM更新要求2(30111)の中に、
広告3011の視聴時間を表す広告視聴時間情報301111が含まれている。

一方、セキュアモジュール302は、Kw2情報30112を受信してからEMM
更新要求2(30111)を受信するまでの時間を測定し、その時間が広告視聴時
10 間情報301111と異なる場合に、EMM3021に設定されているコンテンツの視
聴情報を削除する広告視聴時間判定部3026を備えている。その他の構成は第
2の実施形態(図8)と変わりがない。

この視聴制御装置の動作について、図11を参照して説明する。

まず、再生／放送装置301は、EMM更新要求2(30111)とKw2情報30112
15 とを含む広告3011を再生または放送し、広告が表示される(ステップ4101)。
なお、EMM更新要求2(30111)には、その広告の視聴時間に関する広告視
聴時間情報301111が含まれている。

Kw2情報30112は広告の最初に再生または放送され(ステップ4102)、
Kw2抽出部3024は、Kw2情報30112を受信すると(ステップ4103)、K
20 Kw2情報30112を鍵Kw3022で復号化して、鍵Kw2(3025)を抽出する(ス
テップ4105)。なお、広告視聴時間判定部3026は、Kw2情報30112の受信
時刻を記憶しておく(ステップ4104)。

次に、EMM更新要求2(30111)が広告の最後に再生または放送され(ス
テップ4106)、EMM更新部2(3023)は、EMM更新要求2(30111)を受
25 信すると(ステップ4107)、鍵Kw2(3025)でEMM更新要求2(30111)
復号化し(ステップ4109)、その情報をさらに鍵Kw3022で復号化して、E
MM更新要求2(30111)で指定されているコンテンツを有効期限まで視聴可

能とする情報をEMM3021に設定する。なお、広告視聴時間判定部3026は、EMM更新要求2(30111)の受信時刻を記憶しておく(ステップ4108)。

次に、広告視聴時間判定部3026は、Kw2情報30112を受信してからEMM更新要求2(30111)を受信するまでの時間を測定し、広告視聴時間情報5301111と比較して(ステップ4110)、異なる場合はEMM3021に設定されているコンテンツの視聴情報を削除する一方(ステップ4111)、一致している場合は第2の実施の形態と同様に、EMM更新要求2(30111)で指定されたコンテンツを有効期限まで視聴可能とする情報をEMM3021に設定する(ステップ4112)。

10 その後は、第1の実施形態と同様に、EMM3021に設定されている情報を基にコンテンツの表示を制御する。

このように、この視聴制御装置では、広告の最初と最後とを見た時間間隔を測定するので、広告の早送りなどを防止することができる。

(第4の実施形態)

15 本発明の第4の実施形態では、広告の最初及び最後だけでなく、広告の途中にも一定時間毎にチェックポイントを設け、各チェックポイントの間が早送りをせずに視聴されたことを確認してコンテンツの視聴を可能にする視聴制御装置について説明する。

この装置では、図12に示すように、再生／放送装置401から送出される広告4011に、各チェックポイントで発行される鍵情報Kcm40112と、広告4011の最後で発行されるEMM更新要求2(40111)とが含まれている。鍵情報Kcm40112は、各チェックポイント毎に設定した異なる鍵Kcm4025を暗号化した情報であり、広告の視聴時間中一定時間毎に発行される。最初に発行される鍵情報Kcm40112は、最初のチェックポイントに設定した鍵Kc1を鍵Kw4022で暗号化した情報であり、次に発行される鍵情報Kcm40112は、次のチェックポイントに設定した鍵Kc2を前のチェックポイントに設定した鍵Kc1で暗号化した情報であり、以下同様に、各チェックポイントに設定した鍵

Kcmが、その前のチェックポイントに設定した鍵Kcmで暗号化され、鍵情報Kcm40112として次々と発行される。

また、EMM更新要求2(40111)は、鍵Kw4022で暗号化した後、さらに最後のチェックポイントに設定した鍵Kcm4025で暗号化されている。このEMM更新要求2(40111)には、対象のコンテンツと、そのコンテンツを視聴可能にする有効期間とが記述され、また、各Kcm情報40112の発行時間間隔を表す広告視聴時間情報401111が記述されている。

一方、セキュアモジュール402は、最初に発行されるKcm情報40112を鍵Kw4022で復号化して鍵Kcm4025を抽出し、2番目以降に発行されるKcm情報40112を、1つ前のKcm情報40112から抽出した鍵Kcm4025で復号化して鍵Kcm4025を抽出するKcm抽出部4024と、EMM更新要求2(40111)を受信したときに、Kcm抽出部4024が最後に抽出した鍵Kcm4025を用いてEMM更新要求2(40111)を復号化し、その情報をさらに鍵Kw4022で復号化して、EMM更新要求2(40111)で指定されたコンテンツとそのコンテンツを視聴可能にする有効期間とをEMM4021に設定するEMM更新部4023と、Kcm情報40112を受信してからEMM更新要求2(40111)を受信するまでの各チェックポイント間の時間を測定し、広告視聴時間情報401111と比較して異なる場合はEMM4021に設定されているコンテンツの視聴情報を削除する広告視聴時間判定部4026とを備えている。その他の構成は第2の実施形態(図8)と変わりがない。

この視聴制御装置の動作について、図13を参照して説明する。

まず、再生／放送装置401は、EMM更新要求2(40111)とKcm情報40112とを含む広告4011を再生または放送し、広告4011が表示される(ステップ5101)。なお、EMM更新要求2(40111)には、その広告の視聴時間に関する広告視聴時間情報401111が含まれている。

Kcm情報40112は広告の再生または放送中に順次送出され(ステップ5102)、Kcm抽出部4024は、Kcm情報40112を受信すると(ステップ

5103)、最初に発行されたKcm情報40112を鍵Kw4022で復号化して、鍵Kcm4025を抽出する(ステップ5105)。なお、その際、広告視聴時間判定部4026がKwcm情報40112の受信時刻を記憶する(ステップ5104)。

同様に、2番目以降に発行されたKcm情報40112が広告の再生または放送
5 中に順次送出され(ステップ5106)、Kcm抽出部4024にて受信されると(ス
テップ5107)、1つ前のKcm情報から抽出した鍵Kcm4025を用いて復号
化して、鍵Kcm4025を順次抽出する(ステップ5109)。その際、広告視聴
時間判定部4026が2番目以降に発行されたKcm情報40112の受信時刻を記
憶する(ステップ5108)。広告視聴時間判定部4026は、Kcm情報40112
10 の発行間隔が広告視聴時間情報401111に設定されている発行間隔と異なると
きは、鍵Kcm4025を削除して以降の鍵Kcm4025またはEMM更新要求2
(40111)を復号化できないようにする。

次に、EMM更新要求2(40111)が広告の最後に再生または放送されると
(ステップ5110)、EMM更新部2(4023)はEMM更新要求2(40111)を
15 受信して(ステップ5111)、Kcm抽出部4024が最後に抽出した鍵Kcm4025
を用いてEMM更新要求2(40111)を復号化し(ステップ5113)、さらにそ
の情報を鍵Kw4022で復号化して、EMM更新要求2(40111)に記載された
コンテンツと、その視聴可能にする有効期限とをEMM4021に設定する。なお、
広告視聴時間判定部4026は、EMM更新要求2(40111)の受信時刻を記憶し
20 ておく(ステップ5112)。

次に、広告視聴時間判定部4026は、Kcm情報40112を受信してからEM
M更新要求2(40111)を受信するまでの時間を測定し、広告視聴時間情報
401111と比較して(ステップ5114)、異なる場合はEMM4021に設定され
ているコンテンツの視聴情報を削除する一方(ステップ5115)、一致している
25 場合は第2の実施の形態と同様に、EMM更新要求2(40111)で指定された
コンテンツを有効期限まで視聴可能とする情報をEMM4021に設定する(ステ
ップ5116)。

その後は、第 1 の実施形態と同様に、EMM4021 に設定されている情報を基にコンテンツの表示を制御する。

このように、この視聴制御装置では、早送りなどをすること無く、広告内の複数のポイントをすべて視聴しないとコンテンツを視聴するための鍵が得られない。従って、広告の早送りなどを確実に防止することができ、広告を確実に視聴させることができる。
5

(第 5 の実施形態)

本発明の第 5 の実施形態では、セキュアモジュールの時刻が不正に変更されることを防止した視聴制御装置について説明する。

10 本発明では、広告の視聴により、コンテンツの視聴を許容する有効期限を設定するが、この方式を遂行するためには、期限を管理するセキュアモジュールの時刻が正確でなければならない。セキュアモジュールの時刻は、従来から、例えば、一日に一回、電源が投入された時などに、外部から時刻情報を取得して補正するように構成されているが、この補正時に誤った情報を故意に与えて15 セキュアモジュールの時刻を不正に変更する操作が行われる虞がある。この実施形態の視聴制御装置は、こうした不正を防止する。

この装置は、図 14 に示すように、時刻情報を発信する時刻補正サイト 501 と、時刻補正サイト 501 から時刻情報を受信して、保持している現在時刻の情報を探正するセキュアモジュール 502 とを備えており、時刻補正サイト 501 は、
20 鍵 K_w5012 を保持し、また、時刻情報をセキュアモジュール 502 から送られてきた鍵 K_t 5024 で暗号化して送信する時刻情報作成部 5011 を具備している。

一方、セキュアモジュール 502 は、鍵 K_w5021 を保持し、また、時刻情報を暗号化するための鍵 K_t 5024 をランダムに発生させる鍵発生部 5022 と、時刻補正サイト 501 から受信した時刻情報を復号化して、セキュアモジュール
25 502 の時刻を補正する時刻補正部 5023 とを備えている。

この視聴制御装置の動作について説明する。まず、セキュアモジュール内の現在時刻を補正する際に、鍵発生部 5022 は、ランダムに鍵 K_t 5024 を発生し、

その鍵を鍵K w5021で暗号化して時刻補正サイト501に送信する。

次に、時刻補正サイト501の時刻情報作成部5011は、暗号化された鍵K t
5024を受信すると、鍵K w5021で復号化し、時刻補正サイト501の現在時刻
を、復号化して得られた鍵K t5024で暗号化してセキュアモジュール502へ
5 送信する。

次に、セキュアモジュール502の時刻補正部5023は、受信した時刻情報を
鍵K t5024で復号化して、セキュアモジュールの時刻を補正する。

このように、この視聴制御装置では、セキュアモジュールの時刻を不正に変
更することができない。そのため、コンテンツの視聴の有効期限を正確に管理
10 することができ、また、コンテンツの視聴時に有効な広告を確実に見せること
ができる。

(第6の実施形態)

本発明の第6の実施形態では、広告を見てコンテンツを無料視聴する方法と、
PPVによりコンテンツを有料視聴する方法とを任意に選択できる視聴制御裝
15 置について説明する。

この装置では、図15に示すように、再生／放送装置601が、EMM更新要
求60111を含む広告6011と、コンテンツの視聴権の購入に必要な金額や視聴
権購入の有効期間などの情報を鍵K w6022で暗号化したPPV情報6012とを
送出する。一方、受信装置は、コンテンツの視聴権の購入操作を行う視聴権購
20 入操作部603を備え、また、セキュアモジュール602は、EMM6021、K w
6022、EMM更新部6023の他に、PPV情報6012で指定されたコンテンツ
の視聴権を指定された有効期限内に購入する操作が視聴権購入操作部603で行
われたとき、EMM6021にそのコンテンツの視聴権が購入されたことを設定す
るPPV操作部6024を備えている。EMM更新部6023は、EMM更新要求
25 60111を受信すると、鍵K w6022で復号化して、EMM更新要求60111に記
載されているコンテンツとその視聴可能な有効期限とをEMM6021に設定す
るが、EMM6021にそのコンテンツの視聴権を購入したと設定されている場合

には、この処理を行わない。その他の構成は第1の実施形態（図1）と変わりがない。

この視聴制御装置の動作について説明する。まず、再生／放送装置601はE MM更新要求60111を含む広告6011とPPV情報6012とを再生または放送

5 する。

セキュアモジュール602のPPV操作部6024は、視聴権購入操作部603からコンテンツの視聴権の購入操作があった場合に、そのコンテンツの視聴権の購入に関するPPV情報6012を受信して鍵Kw6022で復号化し、PPV情報6012で規定された視聴権購入の有効期限内に現在時刻が含まれている場合に、

10 EMM6021にそのコンテンツの視聴権を購入したと設定する。

EMM更新部6023は、EMM更新要求60111を受信すると、それを鍵Kw6022で復号化し、そのEMM更新要求60111が、EMM6021にコンテンツの視聴権を購入したと設定されているコンテンツに対するものである時は、そのEMM更新要求60111を破棄する。それ以外のときは、EMM更新要求60111で指定されたコンテンツとそのコンテンツの視聴可能な有効期限との情報をEMM6021に設定する。

その後は、第1の実施形態と同様に、EMM6021に設定されている情報を基にコンテンツの表示を制御する。

このように、この視聴制御装置では、広告を視聴する代わりに、視聴権を購入してコンテンツを視聴することが可能である。この場合、視聴権購入の有効期限を規定することにより、最新のPPV情報で設定した視聴権の購入金額により、購入させることができる。

（第7の実施形態）

本発明の第7の実施形態では、コンテンツの視聴に必要な広告に関する情報を事前に取得することができる視聴制御装置について説明する。

この装置では、図16に示すように、コンテンツを放送する放送装置701が、コンテンツの番組情報を記述したEPG7012を事前に放送し、その後、EMM

更新要求 70111 を含む広告 7011 と、スクランブルされた暗号化済コンテンツ 7013 と、コンテンツのスクランブル鍵及び視聴条件を暗号化した ECM7014 とを放送する。この EPG 7012 には、各コンテンツ毎に、そのコンテンツを視聴するために必要な広告の一覧情報(コンテンツにおける広告の挿入ポイント、

5 及びそのポイントで視聴すべき広告の対応関係を含む) と、コンテンツの視聴が可能な有効期限の情報と、それらの情報が更新された時にその更新された情報が掲載されるサイト情報とが記載された広告関連情報 70121 が含まれている。

放送されるコンテンツを蓄積して再生する蓄積／再生装置 702 は、受信した
10 EPG 7012 から広告関連情報 7024 を抽出して蓄積し、また、受信した、EM
M 更新要求 70211 を含む広告 7021、暗号化済コンテンツ 7022 及び ECM7023
を蓄積する。

この視聴制御装置の動作について説明する。まず、放送装置 701 は EPG
7012 を放送し、蓄積／再生装置 702 は、蓄積すべきコンテンツの EPG 7012
15 から抽出した広告関連情報 7024 を蓄積する。

次に、放送装置 701 は、広告 7011、暗号化済コンテンツ 7013 及び ECM7014
を放送し、蓄積／再生装置 702 は、それぞれを受信して広告 7021、暗号化済
コンテンツ 7022 及び ECM7023 を蓄積する。

この蓄積／再生装置 702 は、第 1 の実施形態(図 1)の再生／放送装置 101
20 として機能し、コンテンツの再生時に、蓄積している広告 7021、暗号化済コンテンツ 7022 及び ECM7023 を出力する。また、有効期間が過ぎて、蓄積している広告ではコンテンツの視聴ができなくなった場合は、広告関連情報 7024 に記載されたサイトから、コンテンツの視聴に必要な最新の広告の情報を取得し、その広告を放送から受信することができる。

25 このように、この視聴制御装置では、コンテンツを視聴するために必要な広告に関する情報を事前に取得することができ、また、広告に関する情報が更新された場合でも、最新の広告を取得するための情報を得ることができる。

(第8の実施形態)

本発明の第8の実施形態では、過去に蓄積したコンテンツやDVDなどのメディアで提供されるコンテンツが視聴される前に、そのコンテンツの視聴に必要な広告を取得する視聴制御装置について説明する。

5 この装置では、図17に示すように、放送装置801が、EMM更新要求80111を含む広告8011と、広告関連情報80121を含むEPG8012とを放送し、蓄積／再生装置802は、過去に蓄積した広告8021、暗号化コンテンツ8022、ECM8023及び広告関連情報8024を保持している。また、蓄積／再生装置802は、過去に蓄積したコンテンツ8022またはDVDなどのメディアで提供されるコンテンツの視聴を予約する予約手段8025と、蓄積されている広告8021及び広告関連情報8024を更新する広告更新手段8026とを備えている。広告更新手段8026は、更新する広告及び広告関連情報を放送装置801または広告発行サイト803から取得する。

10

この視聴制御装置の動作について説明する。まず、視聴者は、予約手段8025で過去に蓄積したコンテンツまたはDVDなどのメディアで提供されるコンテンツの視聴を予約する。

次に、広告更新手段8026は、視聴予約されているコンテンツの蓄積済みの広告関連情報8024から有効期限情報を参照して、視聴予約されている時間がその有効期限後の場合は、放送装置801から放送されているEPG8012を参考し、対象コンテンツの視聴に必要な広告を蓄積するように予約を行い、その予約した時刻に放送される広告8011と広告関連情報80121とを受信して、広告8021と広告関連情報8024とを更新する。

また、広告更新手段8026は、コンテンツの視聴予約時間までに最新の広告8011及び広告関連情報80121が放送されない場合には、ネットワーク経由で、広告発行サイト803に広告8011と広告関連情報80121とを要求し、それらを取得して広告8021と広告関連情報8024とを更新する。

この蓄積／再生装置802は、第1の実施形態（図1）の再生／放送装置101

として機能する。

なお、E P G 8012 はコンテンツの放送予定に関するものでも、広告の放送予定に関するものでも良い。

このように、この視聴制御装置では、過去に蓄積したコンテンツやD V Dなどのメディアで提供されるコンテンツを視聴する際にも、その視聴前に、そのコンテンツの視聴に必要な最新の広告を取得することができる。

(第 9 の実施形態)

本発明の第 9 の実施形態では、コピーしたコンテンツを視聴する際に、広告の視聴を条件とする視聴制御が可能な視聴制御装置について説明する。

この装置では、図 18 に示すように、コンテンツを蓄積して再生する蓄積／再生装置 901 及び 902 が、コンテンツのコピーを制御するコピー制御部 9015 及び 9025 を備えており、蓄積／再生装置 901 から蓄積／再生装置 902 にコンテンツをコピーする場合、コピー元の蓄積／再生装置 901 に蓄積されている、EMM 更新要求 90111 を含む広告 9011、広告関連情報 9014、暗号化済コンテンツ 9012 及び E CM9013 が、コピー先の蓄積／再生装置 902 にコピーされ、EMM 更新要求 90211 を含む広告 9021、広告関連情報 9024、暗号化済コンテンツ 9022 及び E CM9023 として蓄積される。

この視聴制御装置の動作について説明する。まず、コンテンツをコピーする際は、コピー制御部 9025 がコピー制御部 9015 へコンテンツのコピーを依頼するか、もしくは、コピー制御部 9015 からコピー制御部 9025 へコンテンツのコピーの指示を行う。

次に、コピー制御部 9015 は、該当するコンテンツの広告 9011、暗号化コンテンツ 9012、E CM9013 及び広告関連情報 9014 を蓄積／再生装置 902 へ送信する。

次に、コピー制御部 9025 は、受信した情報をそれぞれ広告 9021、暗号化コンテンツ 9022、E CM9023 及び広告関連情報 9024 として蓄積する。

この蓄積／再生装置 902 は、第 1 の実施形態（図 1）の再生／放送装置 101

として機能する。

このように、この視聴制御装置では、コンテンツをコピーするときに、視聴制御で必要となる情報もコピーされるため、コピーしたコンテンツを視聴する際、元のコンテンツと同様に、広告の視聴を条件にコンテンツの視聴を可能に
5 する視聴制御を実行することができる。

(第 10 の実施形態)

本発明の第 10 の実施形態では、グループを構成するコンテンツへの視聴制御情報（EMM更新要求、広告関連情報）を一括管理する視聴制御装置について説明する。

10 グループを構成するコンテンツは、シリーズ番組や同一ジャンルに含まれるコンテンツなどである。広告主は、同一グループのコンテンツが視聴される際に、同一または関連する広告を見せることにより、広告効果の向上を期待している。

この装置では、図 19 に示すように、広告発行サイト 1000 が、グループ毎のコンテンツの視聴に必要な広告に関する広告関連情報と EMM 更新要求とを含むグループ視聴制御情報 1001 と、グループに属するコンテンツに関する情報であるグループ／コンテンツ対応情報 1002 とを保持し、これらの情報からコンテンツ毎に必要な EMM 更新要求 1004 と広告関連情報 1005 とを作成する視聴情報作成部 1003 を備えている。

20 この視聴制御装置の動作について説明する。まず、視聴情報作成部 1003 は、グループ／コンテンツ対応情報 1002 から同一グループに属するコンテンツを特定し、グループ視聴制御情報 1001 に基づいて、それらのコンテンツの各々に必要な EMM 更新要求 1004 と広告関連情報 1005 とを作成する。

コンテンツ毎に設定された EMM 更新要求 1004 及び広告関連情報 1005 は、
25 第 7 の実施形態（図 16）、あるいは、第 8 の実施形態（図 17）の放送装置に送られて、そこで EMM 更新要求を含む広告や広告関連情報を含む EPG が作成される。

このように、この視聴制御装置では、コンテンツの視聴制御の管理をコンテンツ毎に行う必要が無く、多量のコンテンツの視聴制御の管理を容易に行うことができる。

(第 1 1 の実施形態)

5 本発明の第 1 1 の実施形態では、広告の視聴履歴を収集する視聴制御装置について説明する。

この装置では、図 2 0 に示すように、セキュアモジュール 1102 が、EMM 11021、鍵 K w 11022、EMM 更新部 11023 の他に、広告の視聴履歴を保存して広告発行サイト 1101 に報告する履歴情報管理部 11024 を備えており、また、
10 広告発行サイト 1101 は、受信した視聴履歴情報の復号化やその応答の暗号化に使用する鍵 K w 11012 を保持し、広告の視聴履歴を受信して応答を返す広告視聴履歴収集部 11011 を備えている。

履歴情報管理部 11024 は、視聴した広告の情報を蓄積し、セキュアモジュール内の広告の視聴履歴情報の蓄積領域がいっぱいになった時、または一定期間
15 每に、各広告の発行サイト 1101 に各広告の視聴回数を K w 11022 で暗号化して報告する。また、報告の時期に広告の視聴履歴情報を報告することができなかつた場合は、何らかの不正操作が行われたものと見て、以降の広告の視聴によるコンテンツの視聴を不可とする。

この視聴制御装置の動作について説明する。まず、セキュアモジュール 1102 の履歴情報管理部 11024 は、広告の視聴履歴を保存して視聴した広告の情報を蓄積し、一定期間毎に、あるいは、その前にセキュアモジュール内の広告の視聴履歴情報の蓄積領域がいっぱいになった時はそのときに、EMM 更新部 11023 を動作不能に設定して、各広告発行サイト 1101 に各広告の視聴回数を鍵 K w 11022 で暗号化して送信する。

25 次に、広告発行サイト 1101 の広告視聴履歴収集部 11011 は、受信した広告の視聴回数を鍵 K w 11012 で復号化する。そして、その報告が正当と認められるときは、EMM 更新部 11023 を動作可能に設定し、且つ、報告済みの広告視

聴履歴情報を削除するように指示する応答を、鍵Kw11012で暗号化してセキュアモジュール1102に送信する。また、広告発行サイト1101は、収集した広告の視聴回数を基に広告主から広告料を徴収する。

広告発行サイト1101からの応答を受信したセキュアモジュール1102は、それを鍵Kw11021で復号化して、指示に応じた処理を行う。

このように、この視聴制御装置では、偽りの無い広告の視聴状況を把握することができる。また、広告の視聴履歴情報を報告しない場合はコンテンツの視聴をやめさせることができる。

(第12の実施形態)

本発明の第12の実施形態では、広告の視聴履歴を効率的に収集する視聴制御装置について説明する。

この装置では、サンプリング対象の広告の視聴履歴を収集して、その他の広告の視聴状況を判定する。

この装置では、図21に示すように、再生／放送装置1203が outputする広告12031のEMM更新要求120311の中に、その広告の視聴履歴情報を広告発行サイト1201に報告する／しないを示す告知情報1203111が含まれている。各広告の告知情報1203111は、広告発行サイト1201によって設定される。セキュアモジュール1202の履歴情報管理部12024は、「報告する」告知情報1203111が付された広告の視聴履歴のみを広告発行サイト1201に報告する。

広告発行サイト1201は、他の方法で集めた各広告的好感度のランキング情報12013を保持しており、このランキング情報12013を参照して、収集した広告の視聴履歴情報(サンプリングデータ)から、他の広告の視聴状況を判定する。

この視聴制御装置の動作について説明する。まず、再生／放送装置1203は、EMM更新要求120311を含む広告12031を再生または放送する。広告12031は表示装置に表示される。なお、EMM更新要求120311には、その広告の視聴情報を広告発行サイト1201に報告する／しないを示す告知情報1203111が含まれている。

次に、セキュアモジュール 1202 のEMM更新部 12023 は、EMM更新要求 120311 を受信すると鍵K w 12022 で復号化し、EMM更新要求 120311 で指定されたコンテンツを、指定された有効期限まで視聴可能にする情報をEMM 12021 に設定する。その際、視聴した広告の情報を告知情報 1203111 と共に履歴情報管理部 12024 へ保存する。

次に、履歴情報管理部 12024 は、「報告する」告知情報 1203111 が付された広告の視聴回数の情報を広告発行サイト 1201 に送信し、広告発行サイト 1201 の広告視聴履歴収集部 12011 は、これを受信してセキュアモジュール 1202 に応答を返す。この間の動作は、第 1 1 の実施形態における動作と変わりがない。

次に、広告視聴履歴収集部 12011 は、報告された広告 A の視聴回数 a を基に、ランキング情報には記載されているが視聴回数は報告されていない広告 B の視聴回数 b を、広告 A のランキング及び視聴回数 a と、広告 B のランキング及び視聴回数 b との比例計算で算出する。

このように、この視聴制御装置では、効率的に広告の視聴履歴の情報を収集することができる。

(第 1 3 の実施形態)

本発明の第 1 3 の実施形態では、放送されたコンテンツをリアルタイムで視聴する場合に、放送の途中から見始めた人に対して、コンテンツの最後までの視聴を可能にする視聴制御装置について説明する。

生放送番組を途中から見始めた人は、当然、番組の冒頭に放送された広告を見ていない。この場合、広告が視聴されていないからと言って、番組を見せないのは酷である。この視聴制御装置では、こうしたケースを救済する。

この装置では、図 2 2 に示すように、放送装置 1301 が、EMM更新要求 130111 を含む広告 13011 と、各コンテンツの実放送時間と広告の放送時間とを鍵K w 13022 で暗号化した期限付き EMM更新要求 130121 を含む E P G 13012 とを放送する。セキュアモジュール 1302 は、EMM130211、鍵K w 13022、

EMM更新部 13023 の他に、期限付き EMM更新要求 130121 を受信して鍵K w 13022 で復号化し、期限付き EMM更新要求 130121 に記載されているコンテンツを実放送時間の間、そのコンテンツを視聴可能とする情報を EMM 13021 に設定する期限付き EMM更新要求管理部 13024 を備えている。

5 この視聴制御装置の動作について説明する。放送装置 1301 は、暗号化済コンテンツと ECMとともに期限付き EMM更新要求 130121 を含む EPG 13012 を放送し、また、広告の挿入ポイントで EMM更新要求 130111 を含む広告 13011 を放送する。

本放送を途中から視聴した場合に、セキュアモジュール 1302 の期限付き E 10 EMM更新要求管理部 13024 は、EPG 13012 を受信し、その中の期限付き EMM 更新要求 130121 を鍵K w 13022 で復号化して、期限付き EMM更新要求 130121 に記載されているコンテンツを実放送時間の間、視聴可能とする情報を EMM 13021 に設定する。その結果、そのコンテンツの実放送時間が終了するまでは、コンテンツの視聴が可能になる。

15 次に、番組中に挿入された広告 13011 が視聴され、EMM更新部 13023 が EMM更新要求 130111 を受信すると、EMM更新部 13023 は、それを鍵K w 13022 で復号化して、EMM更新要求 130111 に記載されているコンテンツを、EMM更新要求 130111 に記載されている有効期限まで視聴可能とする情報を EMM 13021 に設定する。このとき、EMM 13021 に、期限付き EMM更新要求管理部 13024 により、その有効期限よりも長いコンテンツの視聴時間が既に設定されている場合は、EMM更新要求 130111 に基づく設定を行わない。

20 このように、この視聴制御装置では、本放送の途中から視聴した場合に、コンテンツを最後まで視聴することができる。しかし、放送されたコンテンツを蓄積した場合は、広告を視聴して EMM更新要求により EMMを更新しなければコンテンツの視聴はできない。

(第 14 の実施形態)

本発明の第 14 の実施形態では、本放送を途中から見始めた人に、その後に

挿入される広告をスキップすること無く視聴するように制御する視聴制御装置について説明する。

この装置では、図 2 3 に示すように、放送装置 1401 から放送される E P G 14012 に、各コンテンツの実放送時間と広告の放送時間とを鍵 K w 14022 で暗号化した暗号化広告関連情報 140121 が含まれており、また、セキュアモジュール 1402 は、暗号化広告関連情報 140121 を受けて鍵 K w 14022 で復号化し、暗号化広告関連情報 140121 に記載されているコンテンツを現在時刻から次の広告が放送されるまでの間、視聴可能とする情報を E MM14021 に設定する暗号化広告関連情報管理部 14024 を備えている。その他の構成は第 1 3 の実施形態（図 2 2）と変わりがない。

この視聴制御装置の動作について説明する。放送装置 1401 は、暗号化済コンテンツと E CMとともに暗号化広告関連情報 140121 を含む E P G 14012 を放送し、また、広告の挿入ポイントで E MM 更新要求 140111 を含む広告 14011 を放送する。

本放送を途中から視聴した場合に、セキュアモジュール 1402 の暗号化広告関連情報管理部 14024 は、暗号化広告関連情報 140121 を受信し、鍵 K w 14022 で復号化して、暗号化広告関連情報 140121 に記載されているコンテンツを現在時刻から次の広告が放送されるまでの間、視聴可能とする情報を E MM 14021 に設定する。なお、E MM14021 にそのコンテンツの視聴時間が一度設定された場合は、更新しない。

次に、番組途中に挿入された広告 14011 が視聴され、E MM 更新部 14023 が E MM 更新要求 140111 を受信すると、E MM 更新部 14023 は、それを鍵 K w 14022 で復号化し、E MM 更新要求 140111 に記載されているコンテンツを E MM 更新要求 140111 に記載されている有効時間まで視聴可能とする情報を E MM14021 に設定する。

このように、この視聴制御装置では、本放送の途中から視聴した場合に、次の広告が放送されるまでコンテンツの視聴が可能になり、その後は、広告を視

聴しなければコンテンツを見ることができなくなる。従って、本放送の途中から視聴した場合でもコンテンツを視聴することができ、かつ、視聴開始後は広告の視聴をスキップすることなく視聴させることができる。

(第15の実施形態)

5 本発明の第15の実施形態では、広告の視聴を条件にコンテンツの視聴を可能にする方式を、1個の鍵で暗号化されたコンテンツに対して適用する視聴制御装置について説明する。

コンテンツを1個の鍵で暗号化することは、デジタル著作権管理(DRM)のために広く行われており、インターネット上で販売されるコンテンツの多く
10 は、この方式で暗号化されている。

この実施形態の視聴制御装置は、広告を視聴すれば、1個の鍵で暗号化されたコンテンツが視聴できるようにしており、そうすることで、広告主に効果的な広告の場を提供し、ユーザに無料でコンテンツを見る機会を与えていた。

この装置は、図24に示すように、暗号化済コンテンツを再生または放送する再生／放送装置1501と、コンテンツの復号化を行うセキュアモジュール
1502と、広告及びコンテンツを表示する表示装置1504とを備えている。

再生／放送装置1501は、1個の鍵(Ks Contents)で暗号化された暗号化済コンテンツ15012と、コンテンツの識別番号及びコンテンツの復号化に用いる鍵Ks Contentsの情報を鍵Kw15022で暗号化したKs Contents情報
20 15013と、コンテンツを視聴するために必要な広告15011とを出力する。広告15011には、コンテンツの特定情報及び視聴可能な有効期限が記述されたEMM更新要求150111が含まれており、EMM更新要求150111は鍵Kw15022で暗号化されている。

この広告15011、Ks Contents情報15013及び暗号化コンテンツ15012は、
25 例えばDVDなどの記録媒体に一体に記録されており、再生／放送装置1501は、この記録媒体を再生して広告15011、Ks Contents情報15013及び暗号化コンテンツ15012を出力し、あるいは、再生した情報をネットワークを通じ

て送出する。

セキュアモジュール 1502 は、コンテンツの視聴条件を規定する EMM15021 と、EMM更新要求 150111 及び K s Contents 情報 15013 を復号化するための鍵 K w 15022 とを保持し、EMM更新要求 150111 を鍵 K w 15022 で復号化
5 して、EMM更新要求 150111 に記載されているコンテンツを、EMM更新要求 150111 に記載されている有効期限まで視聴可能にする情報を EMM15021 に設定する EMM更新部 15024 と、K s Contents 情報 15013 を鍵 K w 15022 で復号化して鍵 K s Contents を抽出する K s Contents 抽出部 15025 と、暗号化済コンテンツ 15012 を K s Contents 抽出部 15025 が抽出した鍵 K s
10 Contents で復号化して暗号解除コンテンツ 1503 を出力するデスクランプ 15023 とを備えている。なお、暗号化済コンテンツ 15012 は、一個の鍵 K s Contents で暗号化されているため、その鍵が漏洩すると大きな被害が発生する。そのため、この装置では、デスクランプ 15023 を秘匿性の高いセキュアモジュール 1502 内に設けている。
15 また、表示装置 1504 は、再生／放送装置 1501 から出力された広告 15011 と、セキュアモジュール 1502 から出力された暗号解除コンテンツ 1503 とを表示する。

この視聴制御装置の動作について説明する。まず、再生／放送装置 1501 は、EMM更新要求 150111 を含む広告 15011 と、暗号化済コンテンツ 15012 と、
20 K s Contents 情報 15013 とを再生または放送する。広告 15011 は表示装置 1504 で表示される。

セキュアモジュール 1502 内の EMM15021 は、最初はどのコンテンツも視聴不可能と設定されている。EMM更新部 15024 は、EMM更新要求 150111 を受信すると鍵 K w 15022 で復号化して、EMM更新要求 150111 に記載されているコンテンツを、EMM更新要求 150111 に記載されている有効期限まで視聴可能にする情報を EMM15021 に設定する。
25 次に、K s Contents 抽出部 15025 は、K s Contents 情報 15013 を鍵 K w

15022 で復号化して鍵K s Contents を抽出する。

次に、デスクランプ 15023 は、暗号化済コンテンツ 15012 を受信し、EMM15021 に設定されているそのコンテンツの視聴可能な有効期限と、現在時刻とを比較して、視聴可能な場合に、暗号化済コンテンツ 15012 を鍵K s
5 Contents で復号化して暗号解除コンテンツ 1503 を送出する。表示装置 1504 は、その暗号解除コンテンツ 1503 を表示する。

このように、この視聴制御装置では、ネットワーク上で提供される、一個のキーで暗号化されたコンテンツに対して、最新の広告の視聴を条件としてコンテンツの視聴を許容する視聴制御が可能である。

10 (第 16 の実施形態)

本発明の第 16 の実施形態では、一個のキーで暗号化されたコンテンツの復号キーを安全に受け渡すことができる視聴制御装置について説明する。

ここでは、広告発行サイトが、ネットワーク上で、最新の広告を視聴したユーザにコンテンツを提供する形態を想定しており、このとき、ユーザが広告發
15 行サイトからコンテンツの復号キーを安全に取得できるようにしている。

この装置では、図 25 に示すように、コンテンツを視聴するための鍵K s Contents を発行する広告発行サイト 1601 が、広告発行サイト毎の鍵K s site を暗号化するための鍵K w 16011 を保持し、鍵K s site を鍵K w 16011 で暗号化して K s site 情報 16012 を生成し、コンテンツを視聴するための鍵K s
20 Contents を鍵K s site で暗号化して K s Contents 情報 2 (16013) を生成する。

一方、セキュアモジュール 1602 は、EMM16021、鍵K w 16022、EMM 更新部 16023 の他に、K s site 情報 16012 を鍵K w 16022 で復号化して鍵K s site を抽出する K s site 抽出部 16025 と、K s site 抽出部 16025 が抽出した鍵K s site で K s Contents 情報 2 (16013) を復号化して鍵K s Contents を抽出する K
25 s Contents 抽出部 16024 とを備えている。

この視聴制御装置の動作について説明する。まず、セキュアモジュール 1602 の K s site 抽出部 16025 は、広告発行サイト 1601 から K s site 情報 16012 を取

得し、鍵Kw16022で復号化して鍵Ksiteを抽出する。

次に、セキュアモジュール1602のKsContents抽出部16024は、広告発行サイト1601から、視聴するコンテンツのKsContents情報2(16013)を取得し、鍵Ksiteで復号化して鍵KsContentsを抽出する。

5 このように、この視聴制御装置では、一つのキーで暗号化されているコンテンツのキーを、ネットワーク上で安全に受け渡すことができる。この抽出した鍵KsContentsを使用する視聴制御の様態は、第15の実施形態の場合と同様である。

(第17の実施形態)

10 本発明の第17の実施形態では、蓄積されたコンテンツを一時停止したり、一部を巻き戻したりしてランダムに視聴する場合でも、円滑に視聴制御が可能な視聴制御装置について説明する。

ここでは、広告の挿入ポイントが30分毎に設定されており、コンテンツの冒頭、開始から30分後、開始から1時間後、及び、開始から1時間半後に広告が挿入されるものとする。また、それらの広告のEMM更新要求において、コンテンツ視聴の有効期限が30分間に設定されているものとする。

この場合、広告を視聴することによって、次の広告の挿入時期までのコンテンツの視聴が可能になるため、冒頭の広告から順に正常速度で広告及びコンテンツを再生するならば、コンテンツの最後まで支障なく見ることができる。

20 しかし、コンテンツの再生時に一時停止やスロー再生を行うと、コンテンツ視聴の有効期限が経過しても次の広告が再生されず、コンテンツの視聴が中断されることになる。

この実施形態の視聴制御装置は、こうした事態を回避することができる。

この装置では、図26に示すように、蓄積／再生装置1701が、暗号化済コンテンツ17012、ECM17013、広告関連情報17014(第7の実施形態参照)、EMM更新要求170111を含み各挿入ポイントで挿入される広告17011の他に、コンテンツの再生時に広告関連情報17014に記載されている順に広告の再生

を制御する広告再生制御部 17015 を備えている。その他の構成は第 1 の実施形態（図 1）と変わりがない。

この視聴制御装置の動作について説明する。まず、蓄積／再生装置 1701 は、コンテンツを再生する際に、EMM更新要求 170111 を含む広告 17011（広告 5 関連情報 17014 に記載されている最初の広告 17011）と暗号化済コンテンツ 17012 とを再生する。その時に暗号化済コンテンツ 17012 と同期したECM 17013 も再生する。広告 17011 は表示装置 1706 で表示される。

なお、広告再生制御部 17015 は、再生した広告によって確保された視聴可能な時間が経過しても次の広告が再生されない場合（こうした状態はコンテンツ 10 をランダムに再生する場合に発生する）は、暗号化済コンテンツ 17012 及びECM17013 の再生を止めて、広告関連情報 17014 に記載されている次の広告 17011 を再生させ、その後に暗号化済コンテンツ 17012 及びECM17013 の再生を再開させる。

セキュアモジュール 1702 における動作は、第 1 の実施形態と同じである。
15 広告再生制御部 17015 の制御のもとに、広告 17011 が広告関連情報 17014 に記載されているスケジュールで再生されるため、コンテンツの視聴は、コンテンツがランダムに再生される場合であっても、中断すること無く継続する。

このように、この視聴制御装置では、コンテンツをランダムに視聴する場合でも、コンテンツの視聴の中断を招くこと無く視聴制御を行うことができる。

20 （第 18 の実施形態）

本発明の第 18 の実施形態では、コンテンツがランダムに視聴される場合でも、コンテンツに付与された複数の広告が公平に視聴されるように視聴制御する視聴制御装置について説明する。

コンテンツがランダムに視聴されるときに、広告関連情報に記載されたスケ 25 ジュールで、コンテンツに付与された複数の広告を順番に再生すると、順番の遅い広告は、順番の早い広告に比べて再生の機会が減少する。第 17 の実施形態で示した例で言えば、開始から 1 時間半後に挿入される広告が再生される確

率は、開始から 30 分後に挿入される広告が再生される確率よりも低くなる。

この実施形態の視聴制御装置は、こうした不公平を無くすため、コンテンツがランダムに再生されている間に広告の再生時期が来た場合、コンテンツの再生箇所の直前に挿入されるべき広告を再生するようにしている。

5 この装置では、図 27 に示すように、蓄積／再生装置 1801 が、1 つのコンテンツを、広告を挿入する単位で分割した暗号化済コンテンツ 18012 と、各暗号化済コンテンツ 18012 に対応して分割した ECM18013 と、EMM 更新要求 180111 を含み各挿入ポイントで挿入される複数の広告 18011 と、広告の一覧情報（そのコンテンツの広告の挿入ポイントと、そのポイントで視聴すべき広告の対応関係を含む）を含む広告関連情報 18014 と、広告 18011 が再生されるときに、広告関連情報 18014 を参照して、再生しようとする暗号化済コンテンツ 18012 の直前に再生すべき広告 18011 を選択して、その広告の再生を制御する広告再生制御部 18015 とを備えている。その他の構成は第 1 の実施形態（図 1）と変わりがない。

15 この視聴制御装置の動作について説明する。まず、蓄積／再生装置 1801 は、コンテンツを再生する際に、EMM 更新要求 180111 を含む広告 18011（広告再生制御部 18015 が広告関連情報 18014 を参照して再生しようとする暗号化済コンテンツ 18012 の直前に再生すべきものとして選択した広告 18011）と暗号化済コンテンツ 18012 とを再生する。その時に暗号化済コンテンツ 18012 と同期した ECM18013 も再生する。広告 18011 は表示装置 1806 で表示される。

なお、広告再生制御部 18015 は、再生した広告によって確保された視聴可能な時間が経過しても次の広告が再生されない場合（こうした状態はコンテンツをランダムに再生する場合に発生する）は、暗号化済コンテンツ 18012 及び ECM18013 の再生を止めて、広告関連情報 18014 を参照し、再生しようとする暗号化済コンテンツ 18012 の直前に再生すべき広告 18011 を選択してその広告 18011 を再生させ、その後に暗号化済コンテンツ 18012 及び ECM18013

の再生を再開させる。

セキュアモジュール 1802 における動作は、第 1 の実施形態と同じである。

この装置では、コンテンツがランダムに再生される場合であっても、広告再生制御部 18015 の制御のもとに、コンテンツの視聴の中止が発生しないように
5 広告 18011 が再生される。このとき再生される広告は、再生しようとする暗号化済コンテンツ 18012 の直前に挿入されるべきものであるから、広告の挿入順序による再生機会の多寡は無くなる。

このように、この視聴制御装置では、複数の広告が付与されているコンテンツをランダムに視聴する場合でも、公平に広告を視聴させることができる。

10 なお、各実施形態の再生装置に蓄積されている情報をDVDなどの記録媒体に蓄積すれば、DVDを再生することによって、広告の視聴を条件とするコンテンツの視聴制御が可能になる。例えば、記録媒体に、暗号化されたコンテンツと、そのコンテンツを復号化するための鍵と、広告と、その広告が再生視聴されたときにコンテンツの視聴を許容する有効期限の情報を記録し、あるいは、
15 さらに、有効期限が経過した時点で取得すべき最新の広告の取得先を示す広告関連情報を併せて記録することにより、コンテンツの再生の度に最新の広告が視聴されることになる。そのため、この記録媒体は、新たな広告手段となり得る。

以上の説明から明らかなように、前述の視聴制御装置では、広告を視聴した
20 ときにコンテンツが視聴できるように、コンテンツの視聴制御を行うことができる。そのため、視聴者は、コンテンツを無料で視聴するために、確実に広告を見ることになる。また、広告の視聴で可能になるコンテンツの視聴には有効期限が設定されるため、コンテンツの視聴時点がその有効期限内に含まれるよう
25 に最新の広告を視聴することが必要になる。その結果、広告主の期待に沿った広告の視聴が行われる。また、コンテンツ制作者は、過去に制作したコンテンツを対象として広告料を得ることができる。

また、広告の先頭から最後まで視聴しないとコンテンツを見ることが出来な

いように視聴制御することができ、広告を確実に視聴させることができる。

以上、本発明の視聴制御装置の一形態では、コンテンツの識別情報と当該コンテンツの視聴有効期限を示す視聴条件情報を処理モジュールで保持し、前記視聴条件情報を更新する視聴条件更新情報に対応付けられた広告を再生した場合、前記視聴条件更新情報に基づいて、前記処理モジュールで保持している前記視聴条件情報を更新部により更新し、前記視聴条件情報に基づき前記コンテンツの再生制御をするように構成している。

この構成により、視聴者は、コンテンツを無料で視聴するために、確実に広告を見ることになる。また、広告の視聴で可能になるコンテンツの視聴には有効期限が設定されるため、コンテンツの視聴時点がその有効期限内に含まれるように最新の広告を視聴することが必要になる。その結果、広告主の期待に沿った広告の視聴が行われる。また、コンテンツ制作者は、過去に制作したコンテンツを対象として広告料を得ることができる。

また、処理モジュールをセキュアモジュールで構成している。

この構成により、視聴条件の保持およびその更新をセキュアに行うことができる。

また、前記コンテンツの有効期限を、絶対時刻または相対時刻で指定するよう構成している。

この構成によりコンテンツの有効期限が、絶対時刻または相対時刻で指定可能になる。

また、相対時刻で示される前記コンテンツの有効期限から、広告視聴開始時刻から広告視聴終了時刻のうちの任意の時点または広告取得時刻を基準時刻として、絶対時刻で示される前記コンテンツの有効期限を生成するよう構成している。

この構成により相対時刻指定から絶対時刻指定への変換が可能となる。

また、視聴条件更新情報は、対応付けられた広告の有効期限と、前記有効期限が経過した時点で取得すべき最新の広告の取得先を示す広告関連情報を含む

ことよう構成している。

この構成により、最新の広告情報を取得、提供することが可能となる。

また、前記コンテンツまたは前記広告を、放送、通信または記録メディア経由で取得するよう構成している。

5 この構成によりコンテンツまたは広告を放送、通信または記録メディア経由で取得可能となる。

また、前記コンテンツまたは前記広告を、事前に蓄積するよう構成している。

この構成により、前記コンテンツまたは前記広告を、事前に蓄積し再生することが可能となる。

10 また、前記コンテンツ、前記視聴条件更新情報または前記視聴条件情報は、暗号化するよう構成している。

この構成により、前記コンテンツ、前記視聴条件更新情報または前記視聴条件情報をセキュアに保持することが可能となる。

また、前記広告の再生開始時に共通鍵で暗号化した第1の鍵を処理モジュールに出力し、前記広告の再生終了時に、前記第1の鍵で暗号化した前記視聴条件更新情報を処理モジュールに出力し、処理モジュールでは、前記第1の鍵を共通鍵で復号化し、前記視聴条件更新情報を前記第1の鍵で復号化して前記視聴条件情報を更新するよう構成している。

この構成により、広告の先頭から最後まで視聴しないとコンテンツを見ることが出来ないように視聴制御することができ、広告を確実に視聴させができる。

また、処理モジュールで前記第1の鍵を受信してから前記視聴条件更新情報を受信するまでの経過時間と、前記広告の本来の再生表示時間とが異なるとき、前記視聴条件情報を更新するよう構成している。

25 この構成により、広告の最初と最後とを見た時間間隔を測定するので、広告の早送りなどを防止することができる

また、前記広告の再生開始時に共通鍵で暗号化した第1の鍵を処理モジュール

ルに出力し、以後、前記広告の再生が予め決めた量だけ進捗するごとに、直前に送った鍵で新たな鍵を暗号化して処理モジュールに出力し、前記広告の再生終了時には、その直前に送った鍵で暗号化した前記視聴条件更新情報を処理モジュールに出力し、処理モジュールでは、送られた鍵を順次復号化して再生し、

5 前記視聴条件更新情報をその前に送られた鍵で復号化して前記視聴条件情報を更新するよう構成している。

この構成により、早送りなどをすること無く、広告内の複数のポイントをすべて視聴しないとコンテンツを視聴するための鍵が得られない。従って、広告の早送りなどを確実に防止することができ、広告を確実に視聴させることができ

10 きる。

また、処理モジュールで各鍵を受信してから次の鍵を受信するまでの経過時間、及び、最後の鍵を受信してから前記視聴条件更新情報を受信するまでの経過時間が、前記広告の再生を予め決めた量だけ進捗させるために要する時間と異なるとき、前記視聴条件情報の更新を行わないよう構成している。

15 この構成により、早送りなどをすること無く、広告内の複数のポイントをすべて視聴しないとコンテンツを視聴するための鍵が得られない。従って、広告の早送りなどを確実に防止することができ、広告を確実に視聴させることができる。

また、前記構成において、前記コンテンツを複製するとき、前記コンテンツの視聴を可能にする広告を併せて複製するよう構成している。

この構成により複製したコンテンツを視聴する際にも、広告の視聴を条件とする同様の視聴制御を行うことができる。

また、前記構成において、前記視聴条件情報または前記視聴情報更新情報は、コンテンツのグループに対応付けられることを特徴とする請求項1に記載の視聴制御装置。

この構成により、コンテンツの視聴制御の管理を、コンテンツをグループ化して行うことが可能となる。

また、前記構成において、前記コンテンツを再生するとき、当該前記コンテンツの視聴を可能にする広告を、当該コンテンツより前に再生することを特徴とする請求項1に記載の視聴制御装置。

この構成によりコンテンツの視聴を可能にする広告を、コンテンツより前に
5 再生することが可能となる。

本明細書は、2003年6月19日出願の特願2003-174785と、
2004年6月15日出願の特願2004-177584に基づくものである。
この内容をここに含めておく。

10 産業上の利用可能性

本発明にかかる視聴制御装置、視聴制御プログラム、セイキュアデバイスは、
広告を視聴したときにコンテンツが視聴できるように、コンテンツの視聴制御
を行うことができ、そのため、視聴者は、コンテンツを無料で視聴するために、
確実に広告を見ることになるという効果を有し、放送されたコンテンツや蓄積
15 されたコンテンツの視聴を制御する視聴制御装置、視聴制御プログラム、セイ
キュアデバイスとして有用である。

請求の範囲

1. コンテンツの識別情報と当該コンテンツの視聴有効期限を示す視聴条件情報を処理モジュールで保持し、
前記視聴条件情報を更新する視聴条件更新情報に対応付けられた広告を再生
5. した場合、前記視聴条件更新情報に基づいて、前記処理モジュールで保持している前記視聴条件情報を更新部により更新し、前記視聴条件情報に基づき前記コンテンツの再生制御することを特徴とする視聴制御装置。
10. 2. 前記処理モジュールはセキュアモジュールであることを特徴とする請求項
1に記載の視聴制御装置。
15. 3. 前記コンテンツの有効期限は、絶対時刻または相対時刻で指定されることを特徴とする請求項 1に記載の視聴制御装置。
4. 相対時刻で示される前記コンテンツの有効期限から、広告視聴開始時刻から広告視聴終了時刻のうちの任意の時点または広告取得時刻を基準時刻として、絶対時刻で示される前記コンテンツの有効期限を生成することを特徴とする請求項 3に記載の視聴制御装置。
15. 5. 視聴条件更新情報は、広告の有効期限と、前記有効期限が経過した時点で取得すべき最新の広告の取得先の情報を含むことを特徴とする請求項 1に記載の視聴制御装置。
20. 6. 前記コンテンツまたは前記広告を、放送、通信または記録メディア経由で取得することを特徴とする請求項 1に記載の視聴制御装置。
7. 前記コンテンツまたは前記広告を、事前に蓄積することを特徴とする請求項 1に記載の視聴制御装置。
8. 前記コンテンツ、前記視聴条件更新情報または前記視聴条件情報は、暗号化されていることを特徴とする請求項 1に記載の視聴制御装置。
25. 9. 前記広告の再生開始時に共通鍵で暗号化した第 1 の鍵を処理モジュールに出力し、前記広告の再生終了時に、前記第 1 の鍵で暗号化した前記視聴条件更新情報を処理モジュールに出力し、処理モジュールでは、前記第 1 の鍵を共通

鍵で復号化し、前記視聴条件更新情報を前記第1の鍵で復号化して前記視聴条件情報を更新することを特徴とする請求項1に記載の視聴制御装置。

10. 処理モジュールで前記第1の鍵を受信してから前記視聴条件更新情報を受信するまでの経過時間と、前記広告の本来の再生表示時間とが異なるとき、
5 前記視聴条件情報の更新を行わないことを特徴とする請求項9に記載の視聴制御装置。

11. 前記広告の再生開始時に共通鍵で暗号化した第1の鍵を処理モジュールに出力し、以後、前記広告の再生が予め決めた量だけ進捗するごとに、直前に送った鍵で新たな鍵を暗号化して処理モジュールに出力し、前記広告の再生終了時には、その直前に送った鍵で暗号化した前記視聴条件更新情報を処理モジュールに出力し、処理モジュールでは、送られた鍵を順次復号化して再生し、前記視聴条件更新情報をその前に送られた鍵で復号化して前記視聴条件情報を更新することを特徴とする請求項9に記載の視聴制御装置。
10

12. 処理モジュールで各鍵を受信してから次の鍵を受信するまでの経過時間、
15 及び、最後の鍵を受信してから前記視聴条件更新情報を受信するまでの経過時間が、前記広告の再生を予め決めた量だけ進捗させるために要する時間と異なるとき、前記視聴条件情報の更新を行わないことを特徴とする請求項11に記載の視聴制御装置。

13. 前記コンテンツを複製するとき、前記コンテンツの視聴を可能にする広告を併せて複製することを特徴とする請求項1に記載の視聴制御装置。
20

14. 前記視聴条件情報または前記視聴情報更新情報は、コンテンツのグループに対応付けられることを特徴とする請求項1に記載の視聴制御装置。

15. 前記コンテンツを再生するとき、当該前記コンテンツの視聴を可能にする広告を、当該コンテンツより前に再生することを特徴とする請求項1に記載
25 の視聴制御装置。

16. コンピュータを、
コンテンツの識別情報と当該コンテンツの視聴有効期限を示す視聴条件情報

を保持し、

前記視聴条件情報を更新する視聴条件更新情報に対応付けられた広告を再生した場合、前記視聴条件更新情報に基づいて、保持している前記視聴条件情報を更新し、

- 5 前記視聴条件情報に基づき前記コンテンツの再生制御するよう機能させることを特徴とする視聴制御プログラム。

17. 視聴対象の暗号化済コンテンツとその暗号化済コンテンツの視聴可能な有効期限とを指定するコンテンツの視聴条件情報を保持し、前記視聴条件情報で指定された有効期限に基づき前記暗号化済コンテンツを復号化して再生させ

- 10 るセキュアモジュールであって、

前記視聴条件情報で指定された前記暗号化済コンテンツの有効期限を更新する視聴条件更新情報が対応付けられた広告が再生された場合、前記視聴条件更新情報に基づいて前記視聴条件情報を更新し、前記視聴条件更新情報で指定された前記暗号化済コンテンツの視聴を可能にすることを特徴とするセキュアモ

- 15 ジュール。

1/26

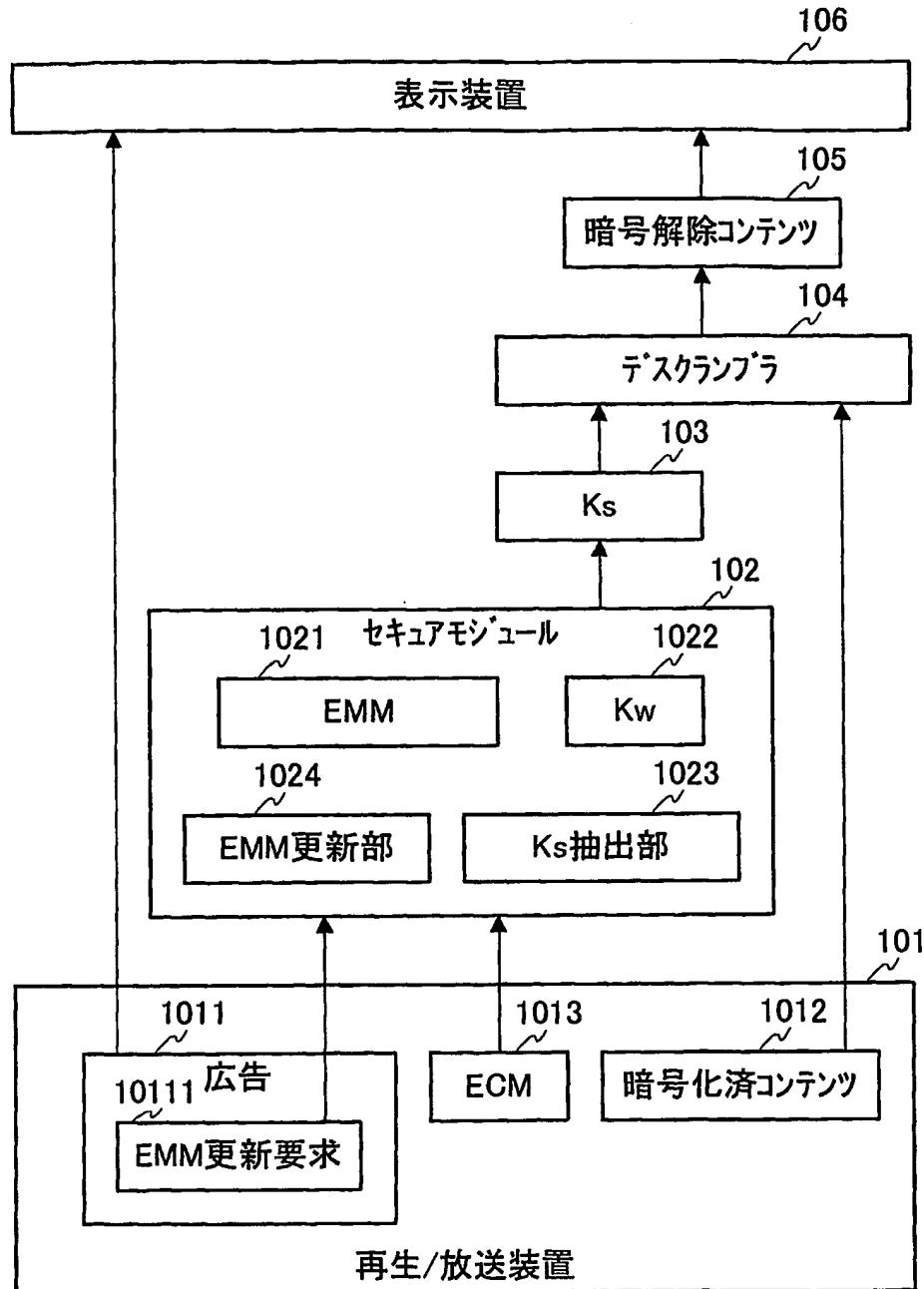


図1

2/26

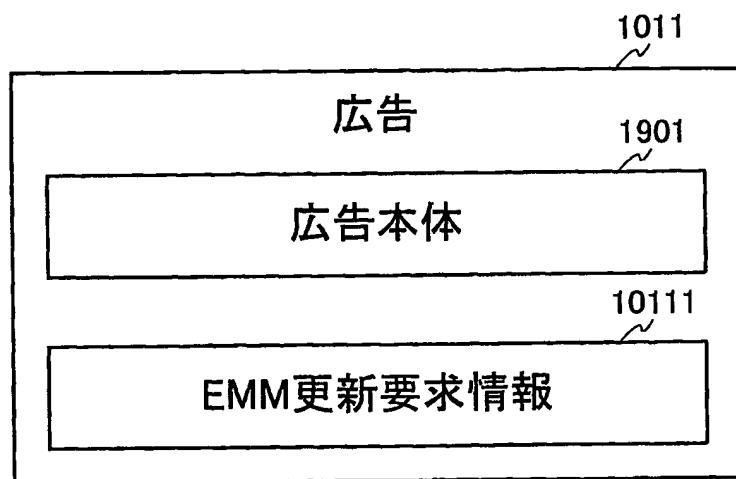


図2

3/26

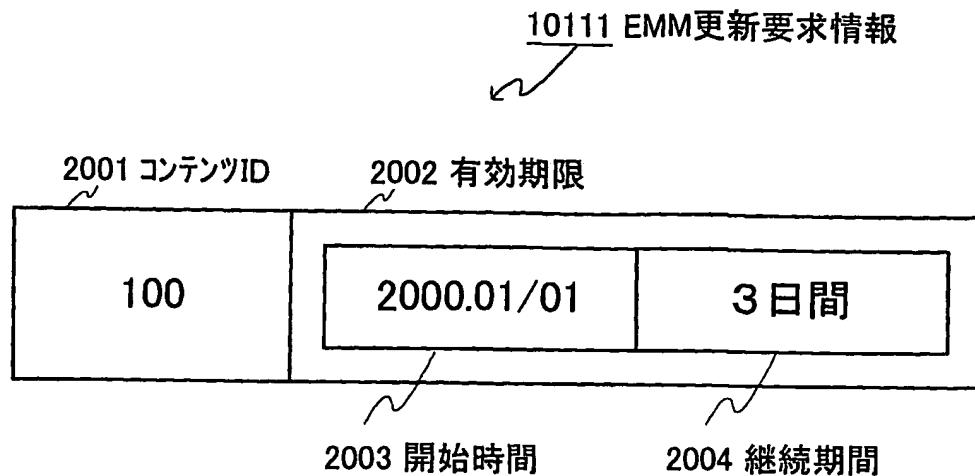


図3

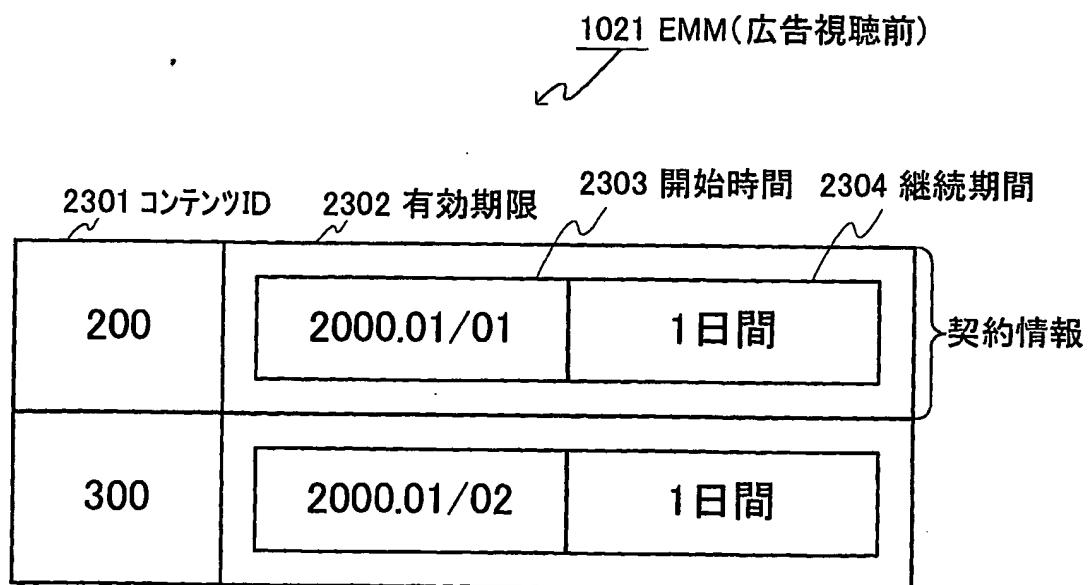


図4

4/26

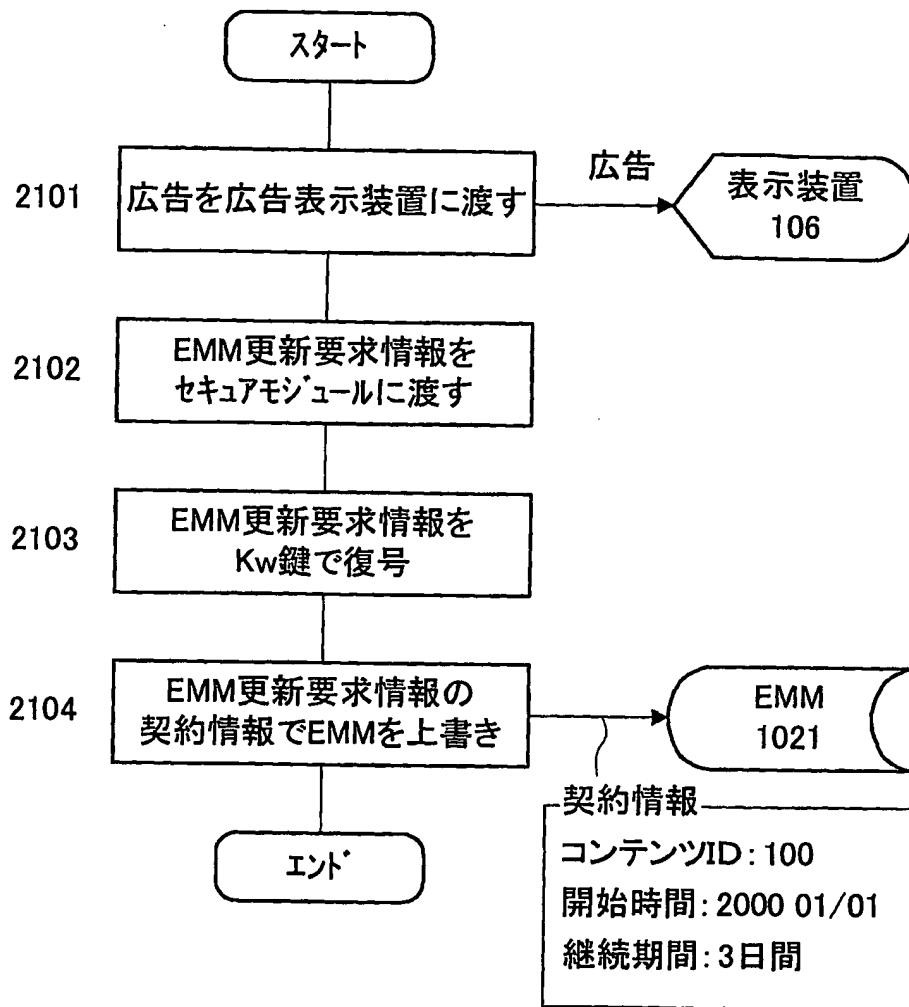


図5

5/26

1021 EMM(広告視聴後)

	2301 コンテンツID	2302 有効期限	2303 開始時間	2304 継続期間	契約情報
200		2000.01/01	1日間		
300		2000.01/02	1日間		
100		2000.01/01	3日間		

図6

6/26

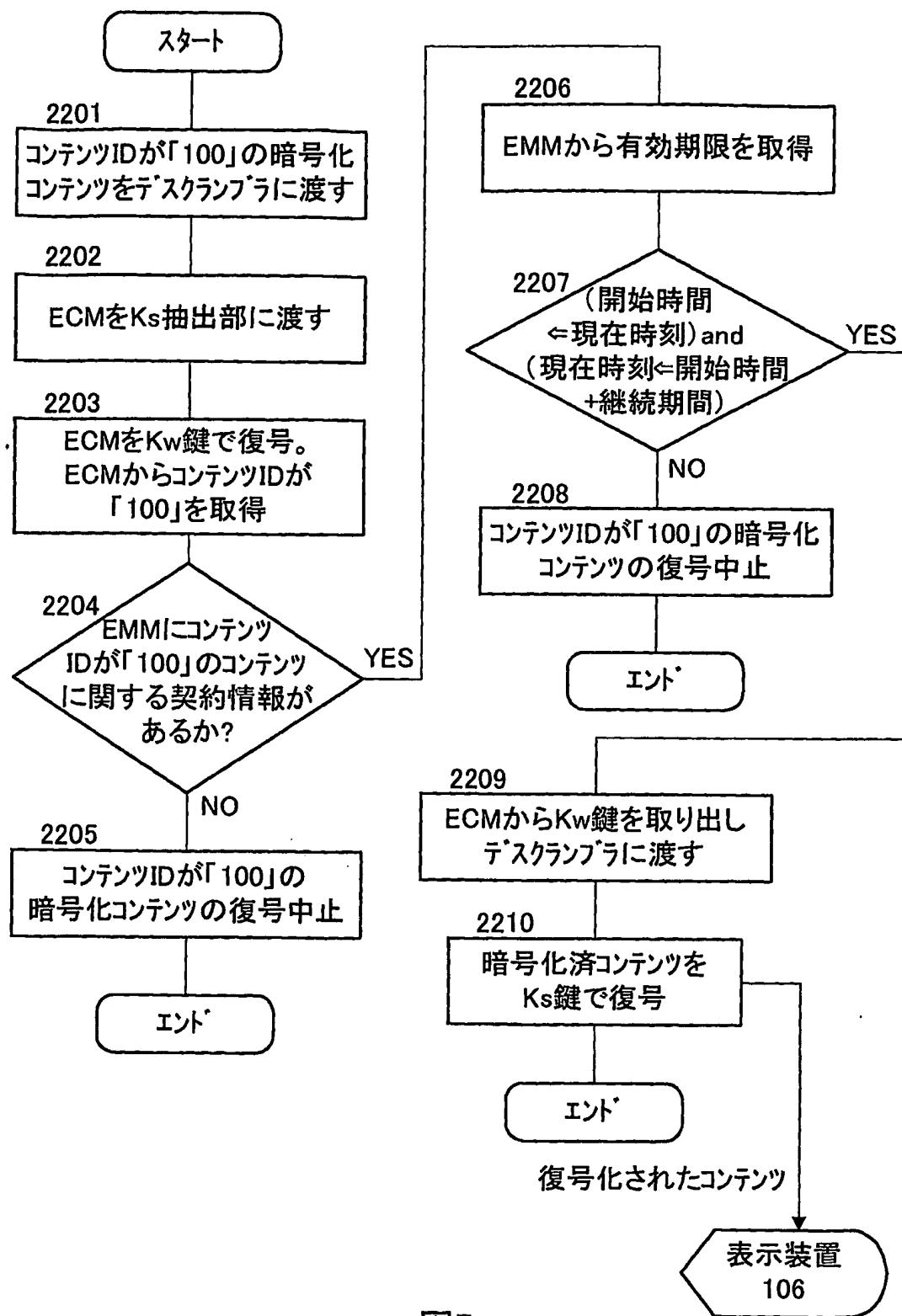


図7

7/26

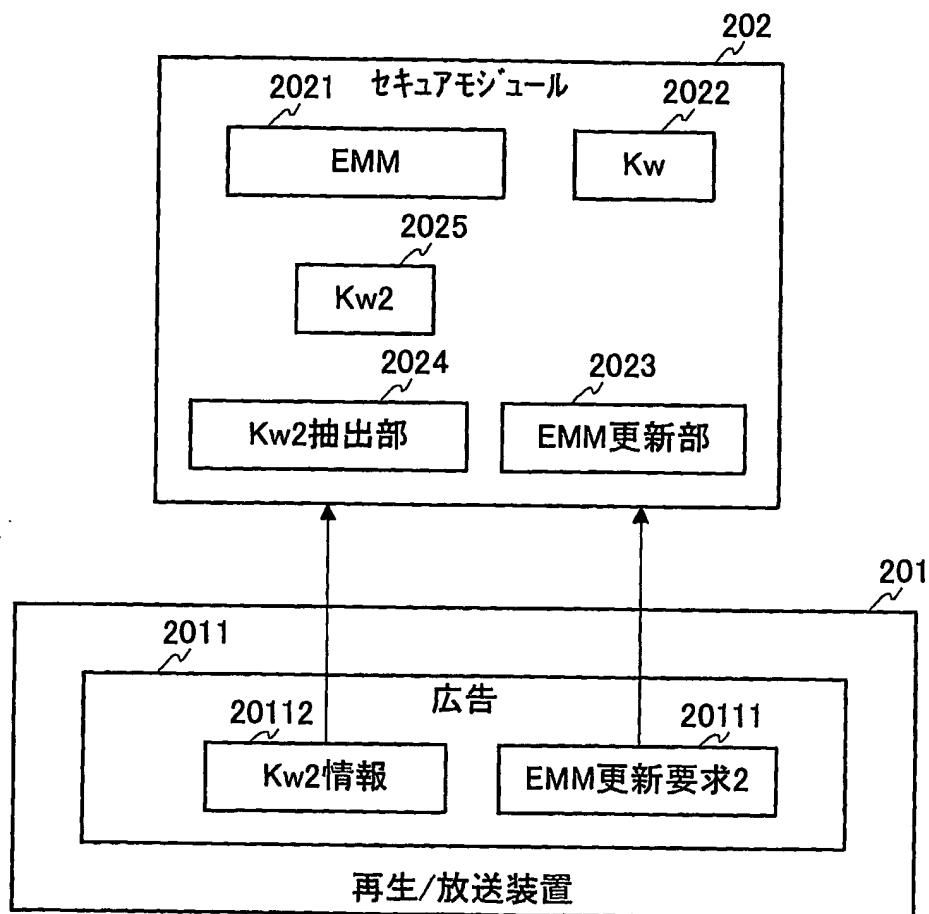


図8

8/26

<再生/放送装置201>

<セキュアモジュール202>

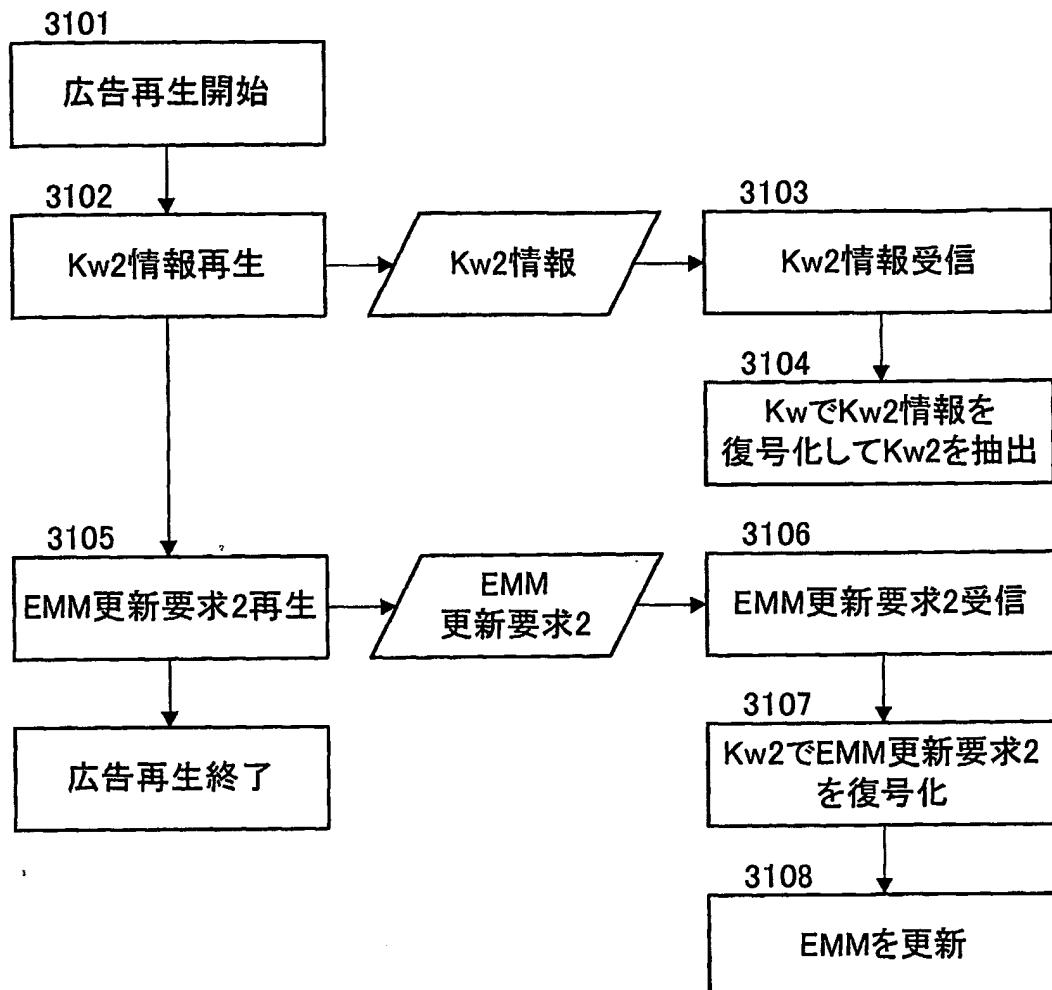


図9

9/26

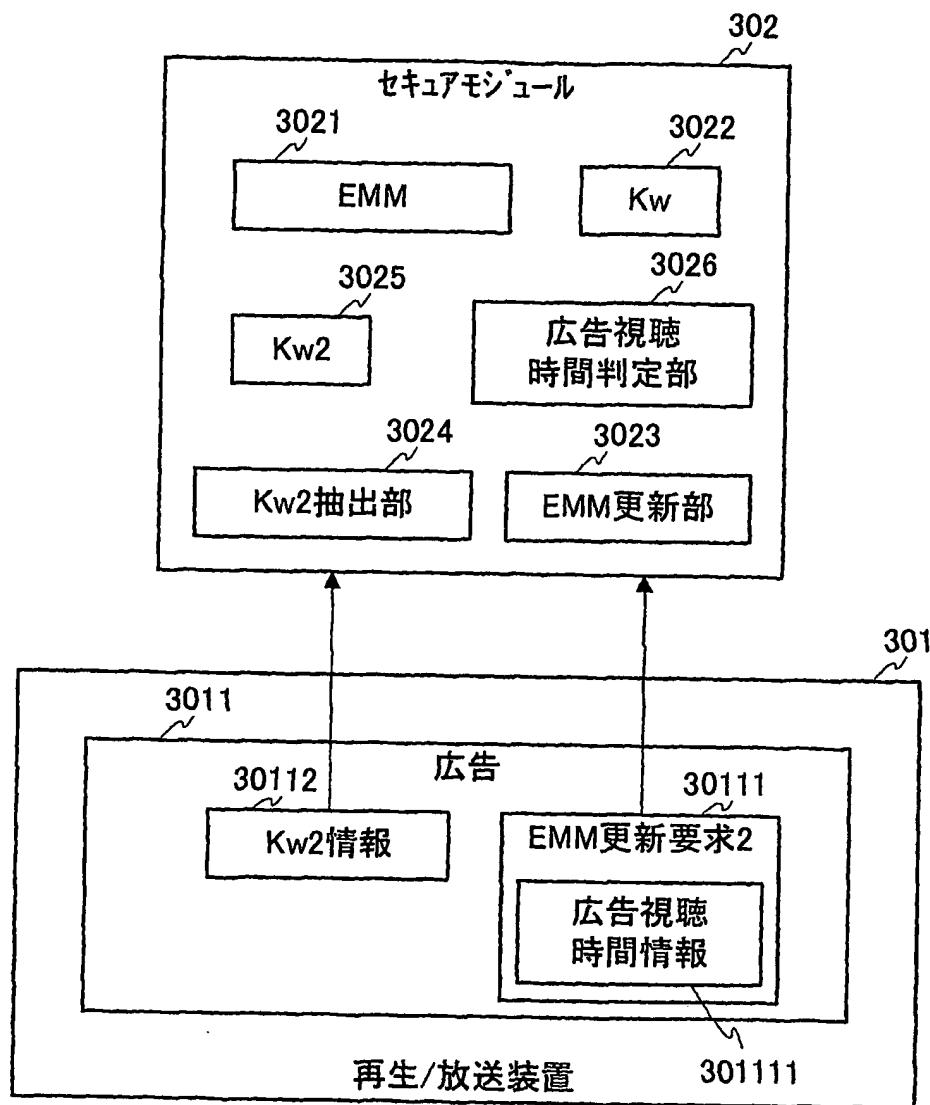


図10

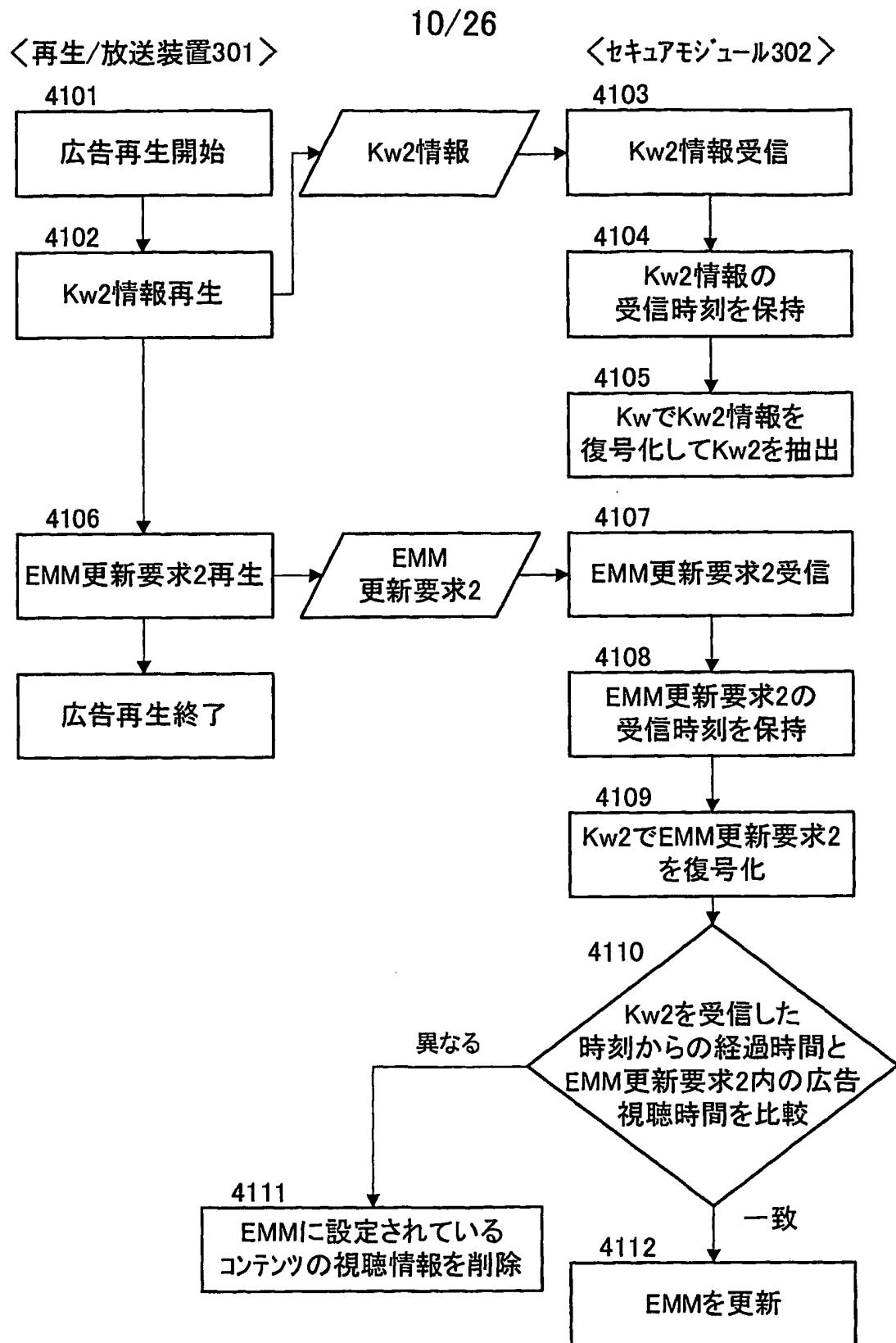


図11

11/26

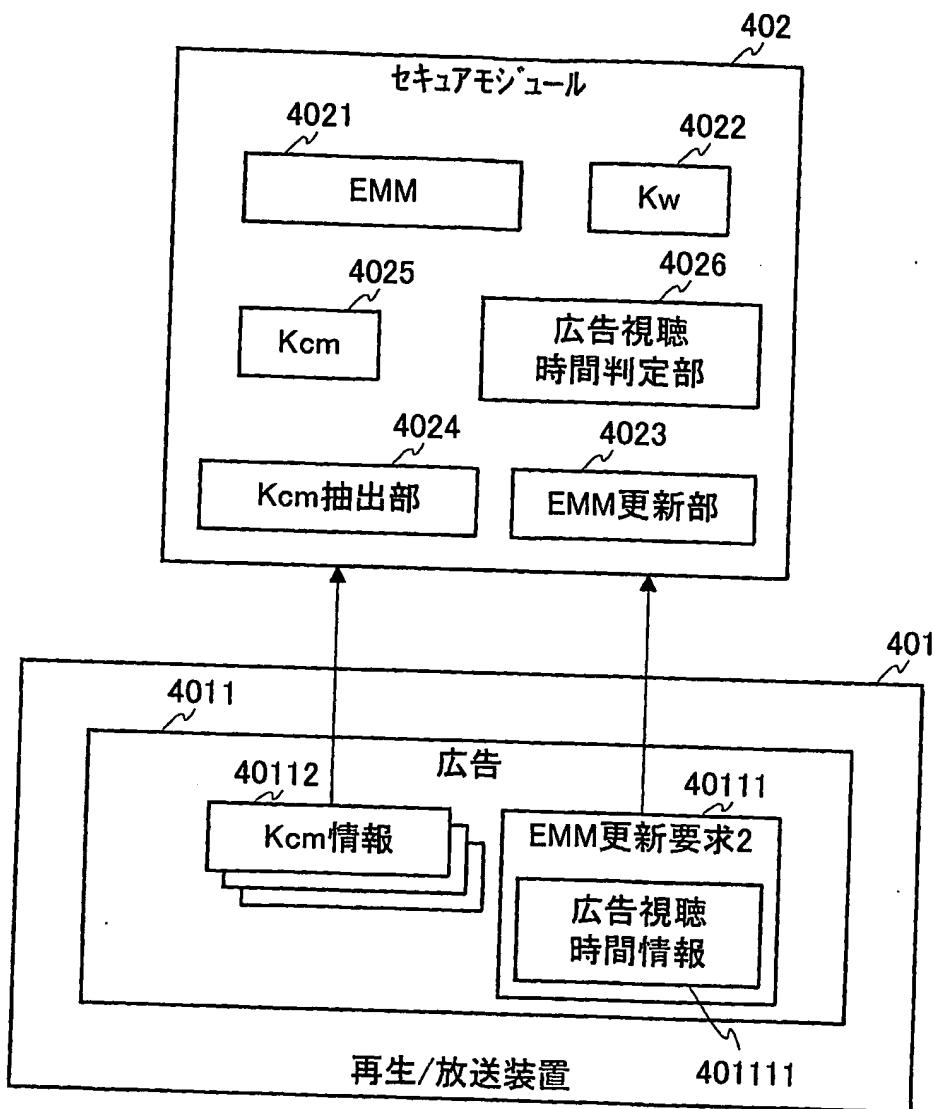
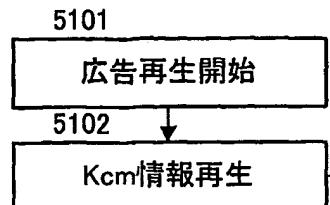


図12

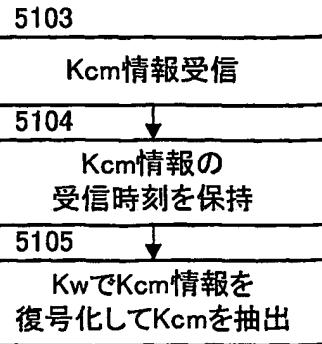
12/26

〈再生/放送装置401〉

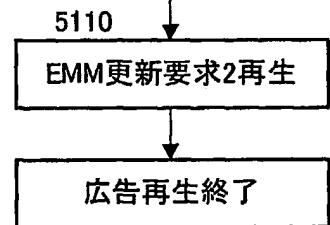
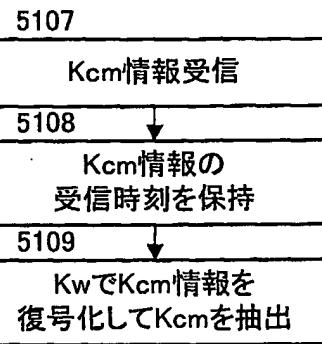
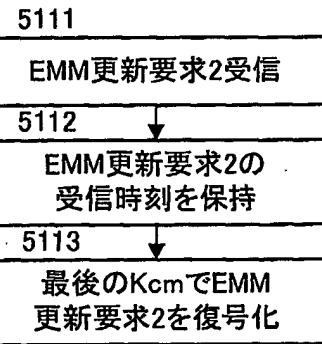


Kcm情報

〈セキュアモジュール402〉



Kcm情報

EMM
更新要求2

5114
Kcmを受信した時刻からの経過時間とEMM更新要求2内の広告視聴時間を比較

異なる

5115
一致
EMMに設定されているコンテンツの視聴情報を削除

5116
EMMを更新

図13

13/26

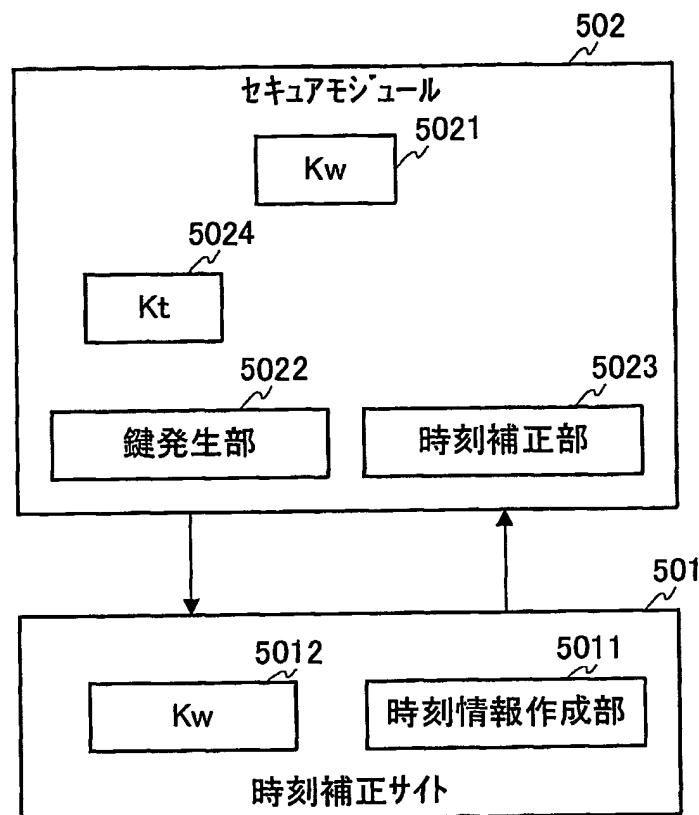


図14

14/26

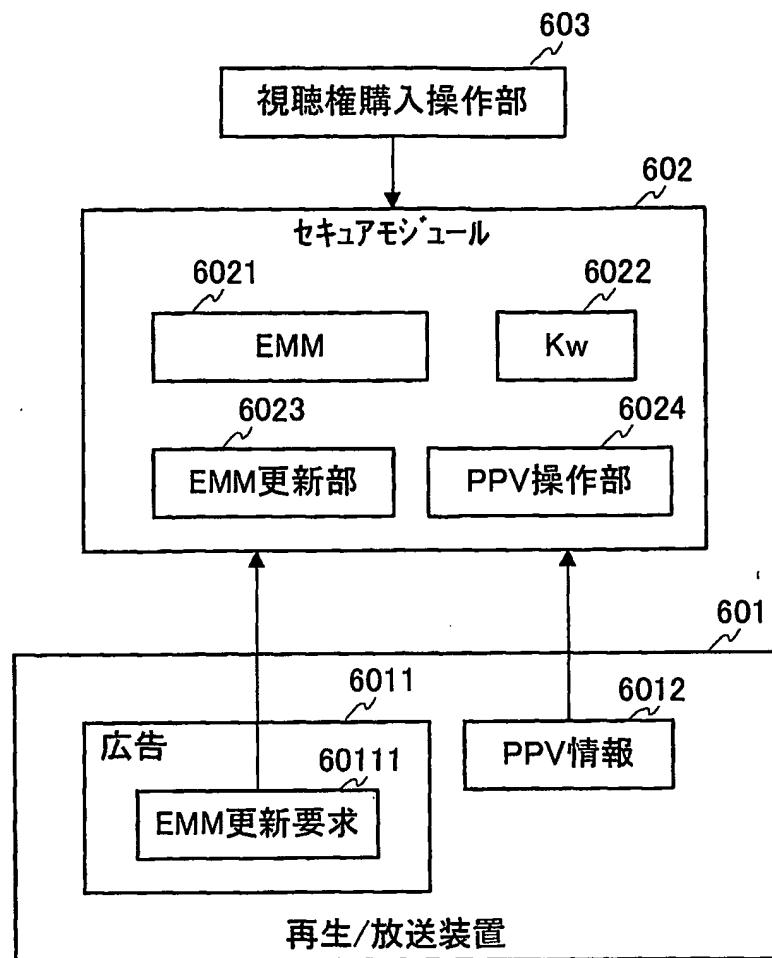


図15

15/26

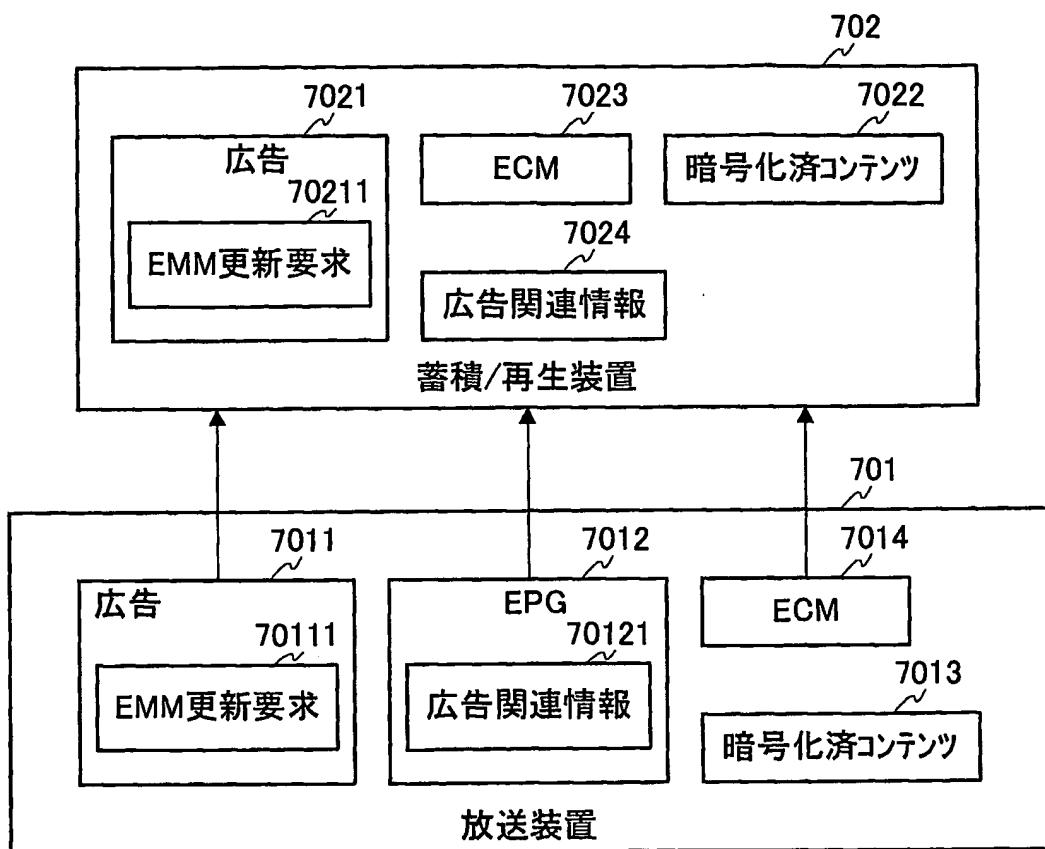


図16

16/26

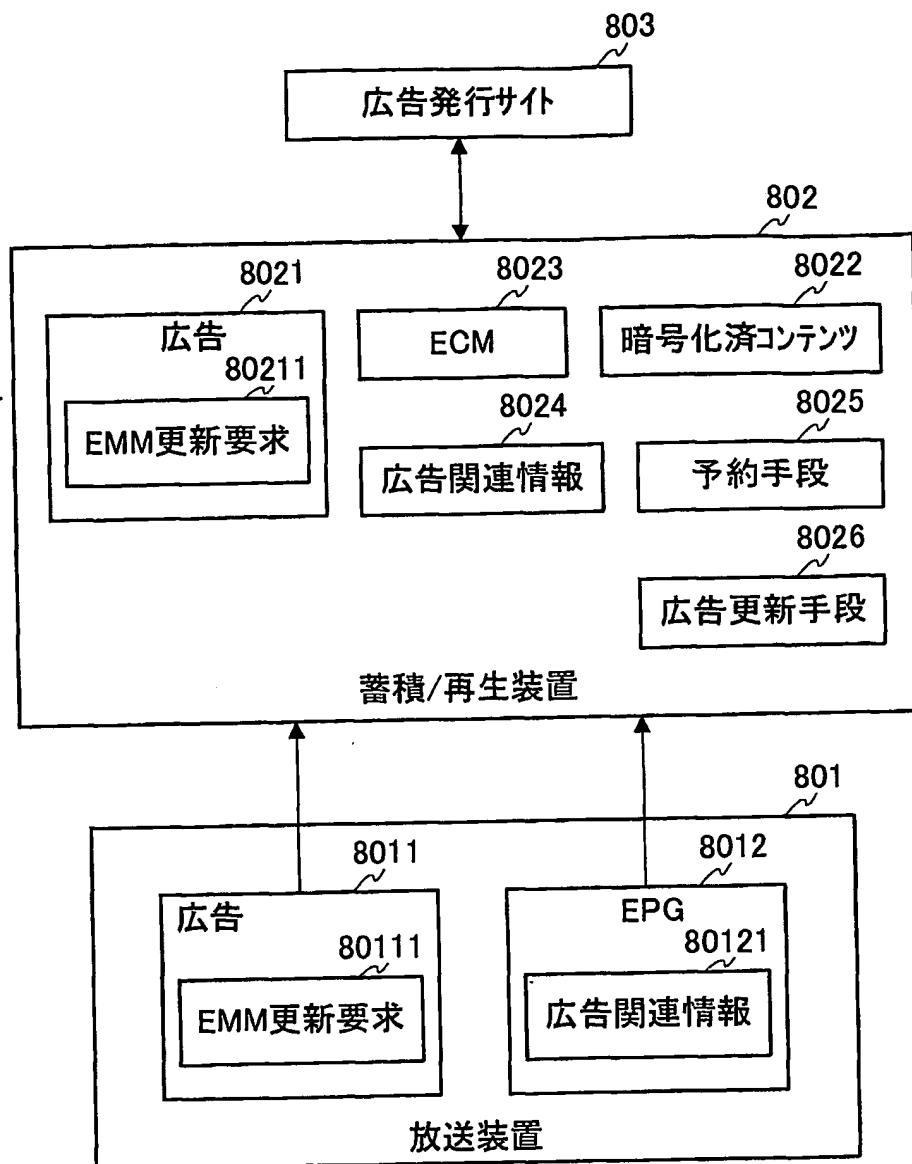


図17

17/26

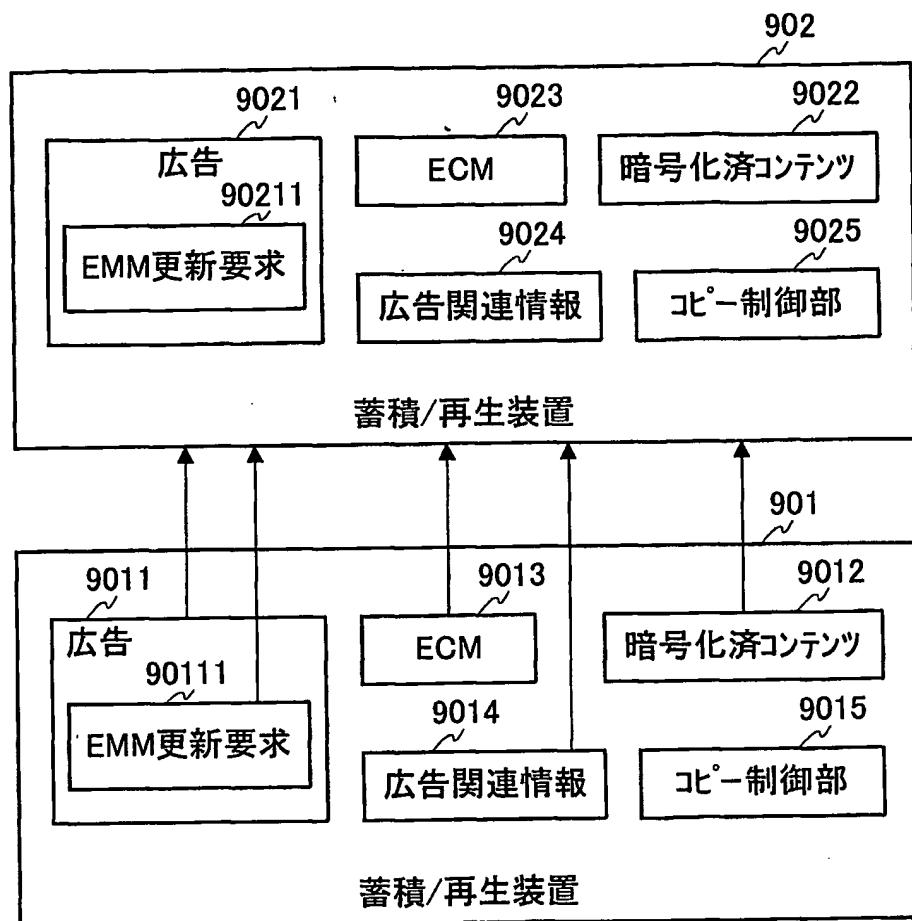


図18

18/26

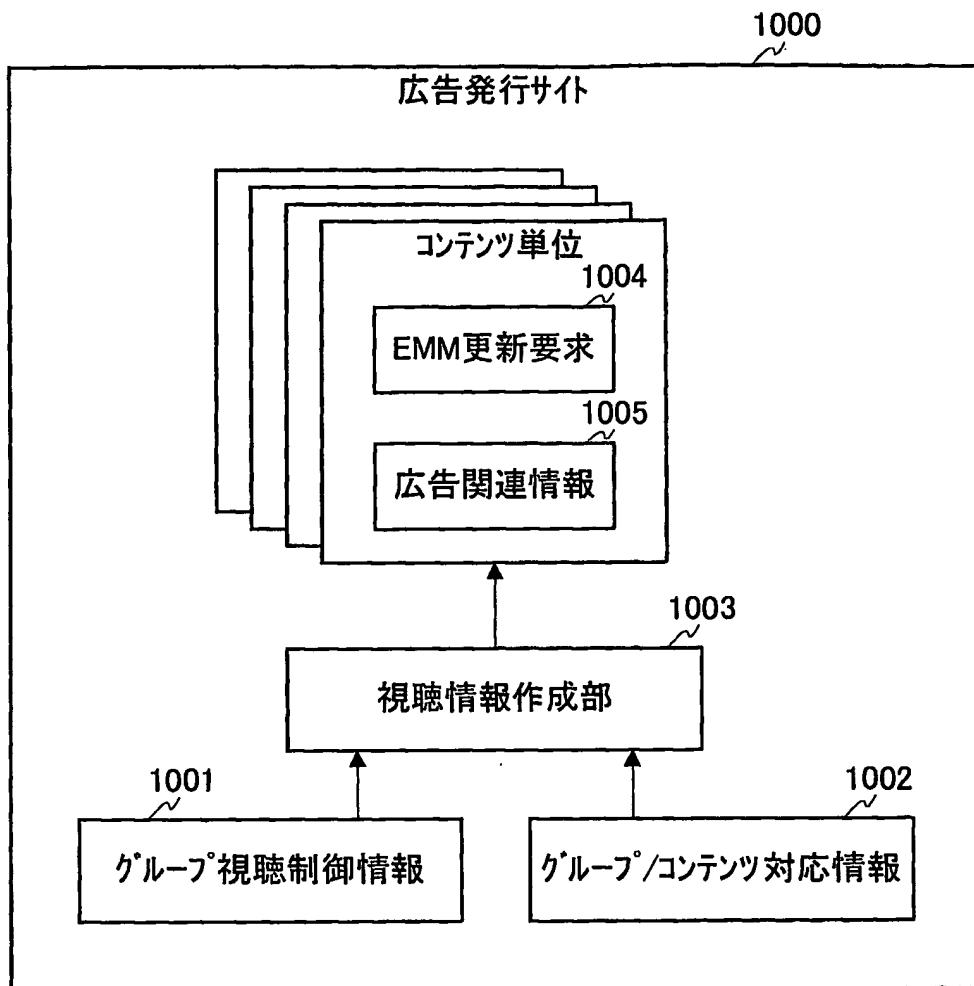


図19

19/26

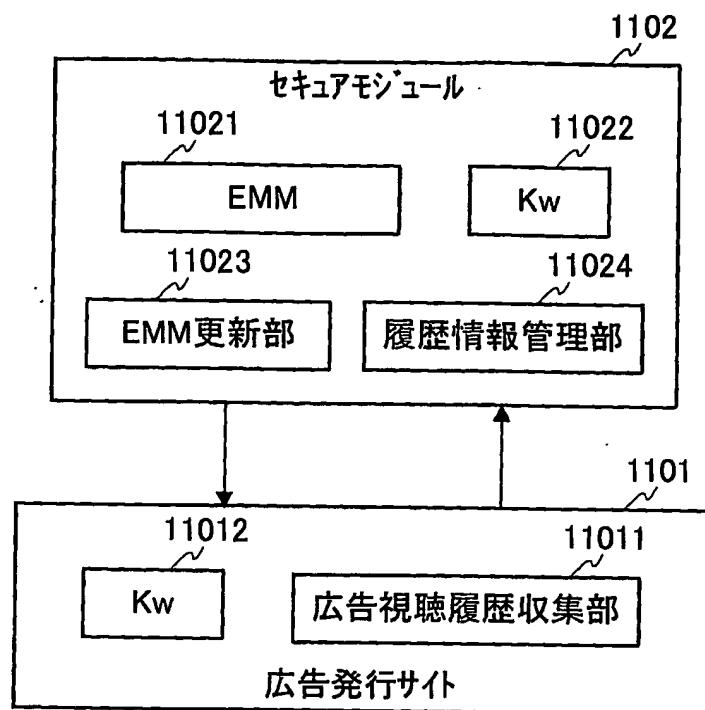


図20

20/26

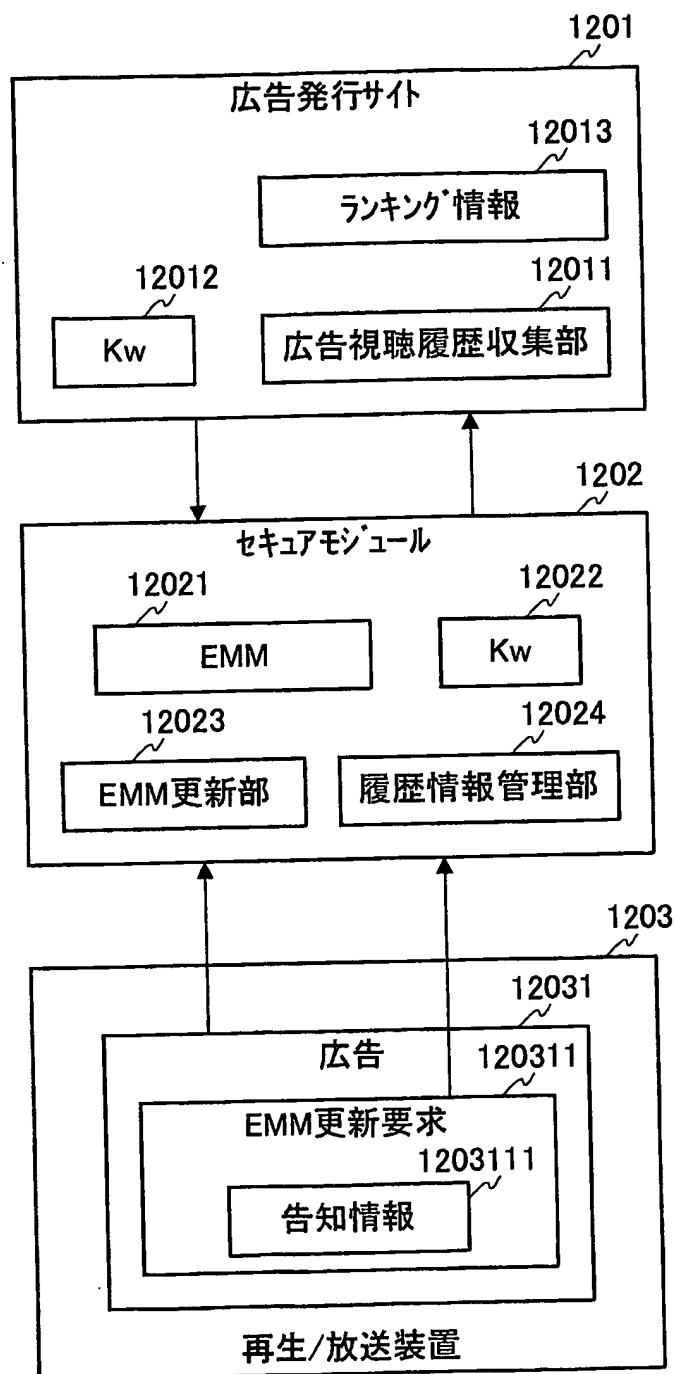


図21

21/26

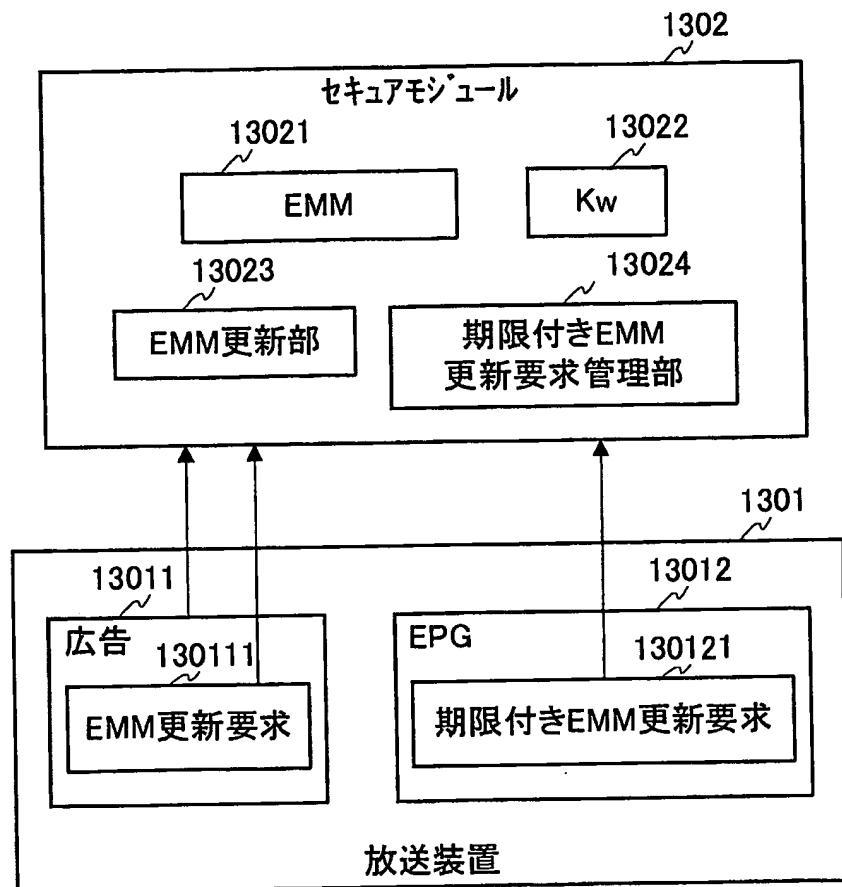


図22

22/26

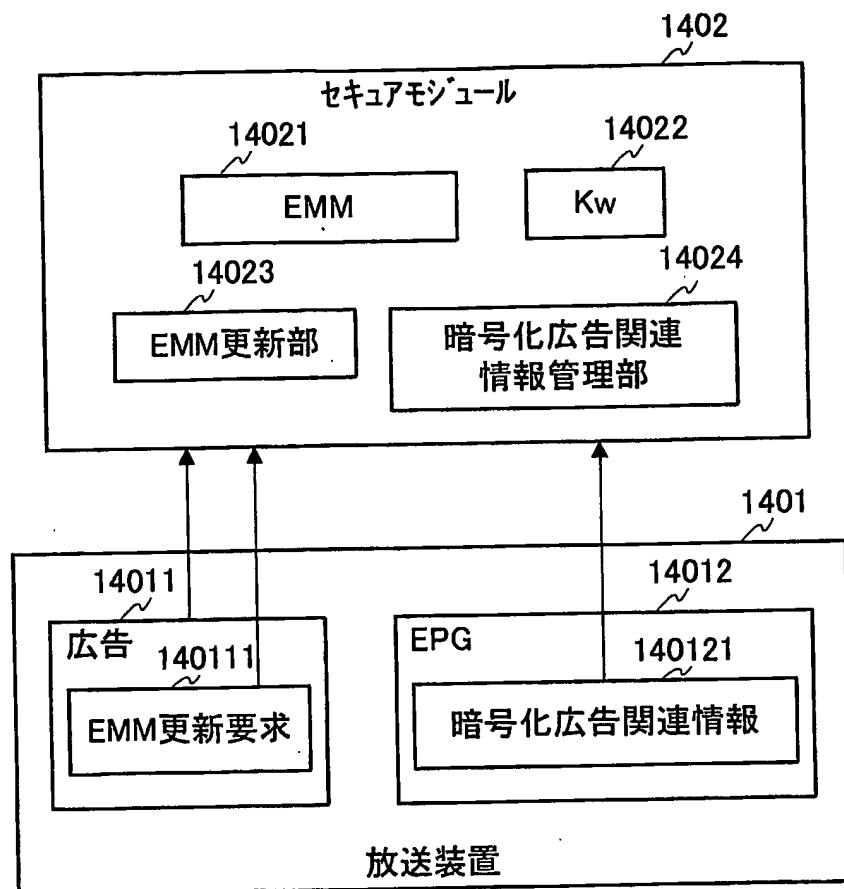


図23

23/26

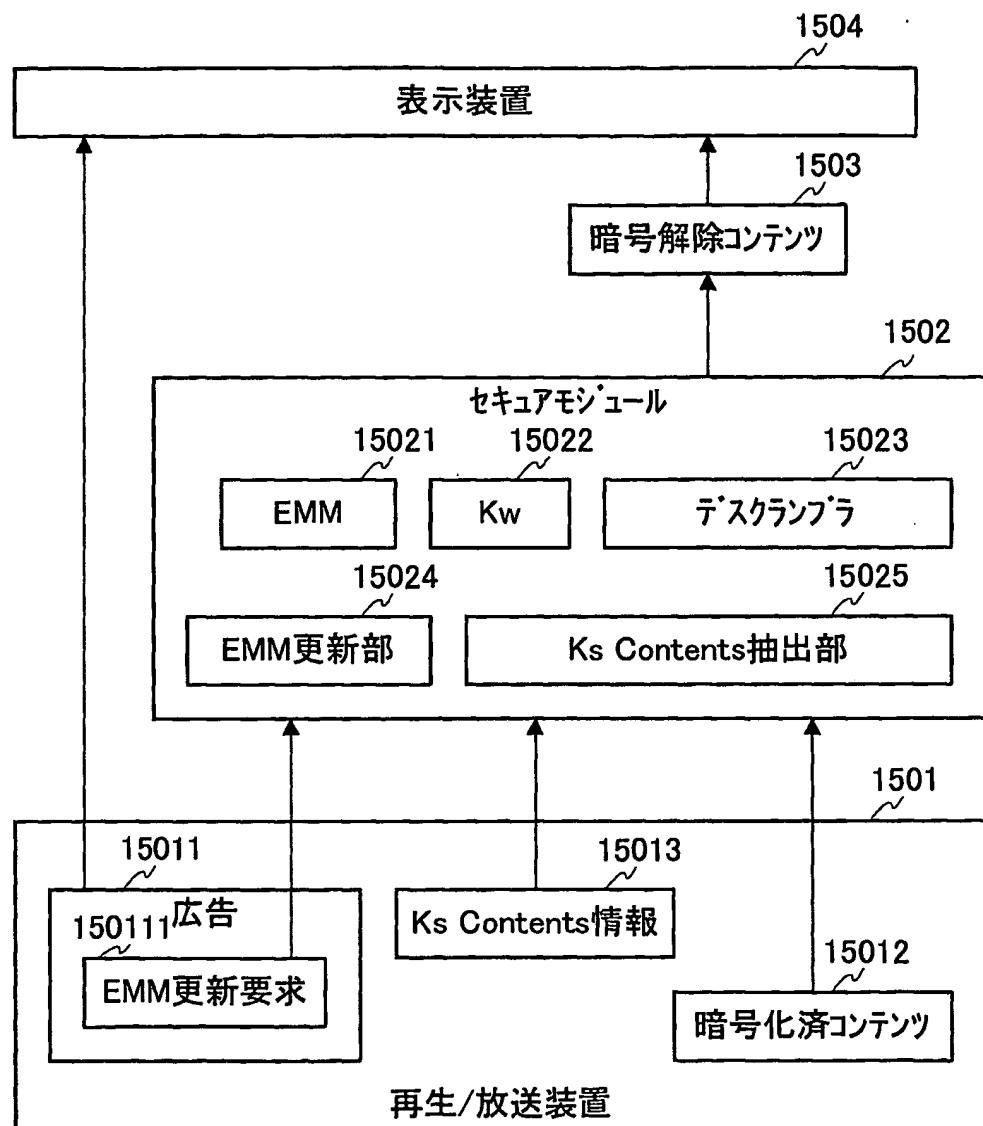


図24

24/26

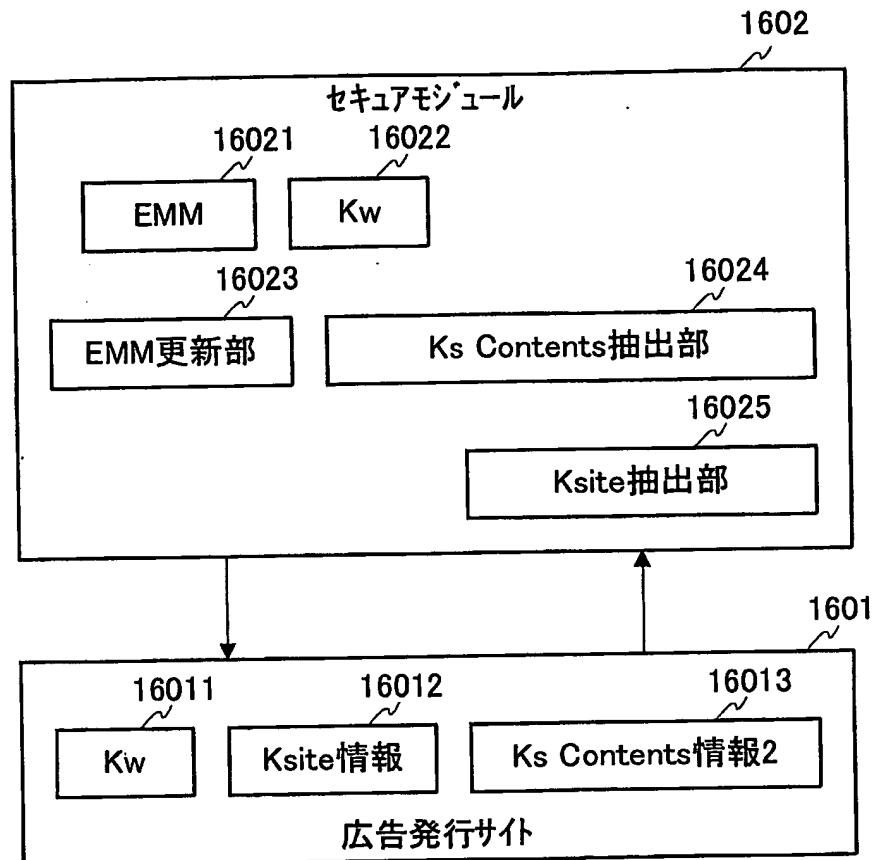


図25

25/26

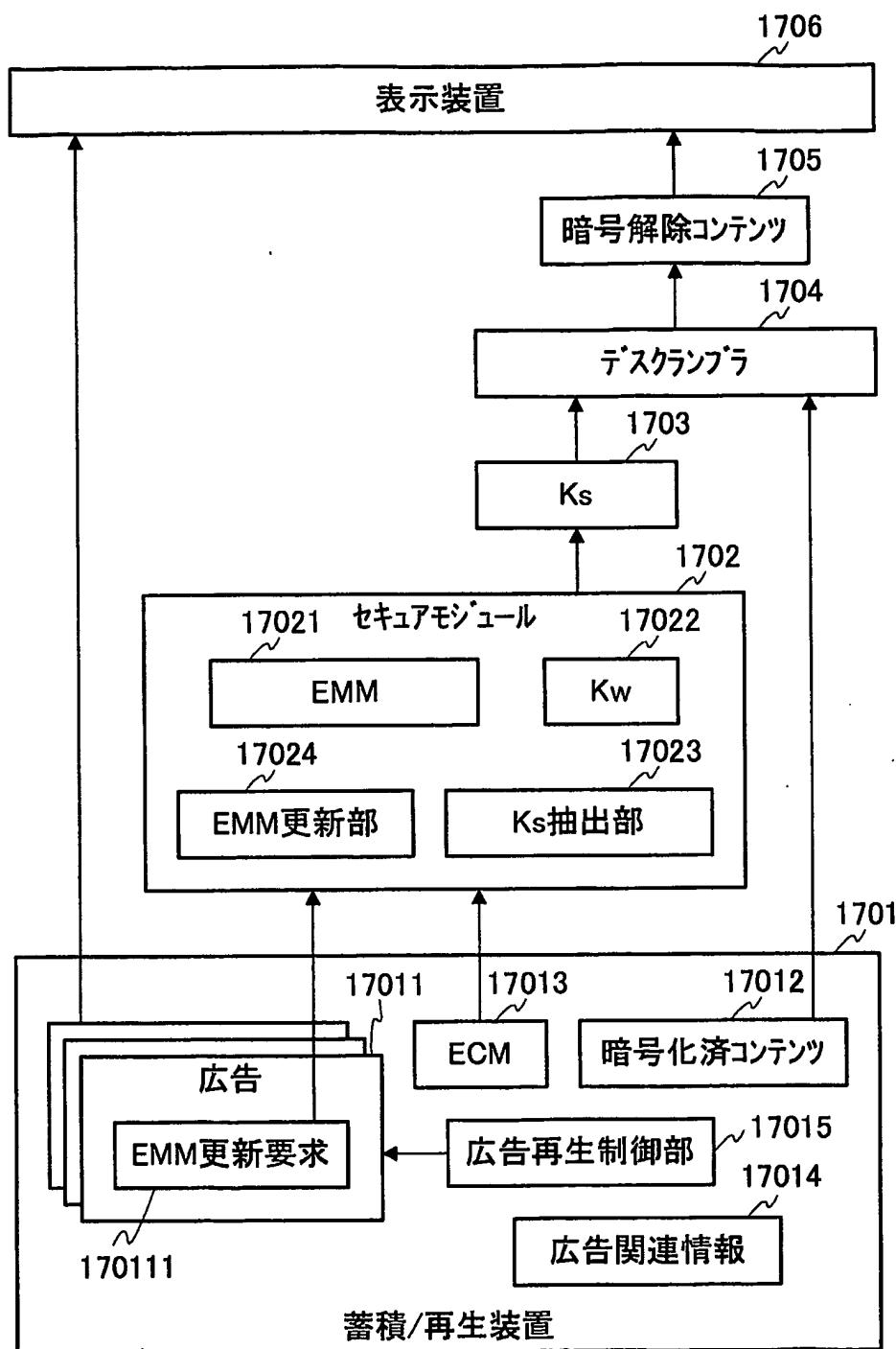


図26

26/26

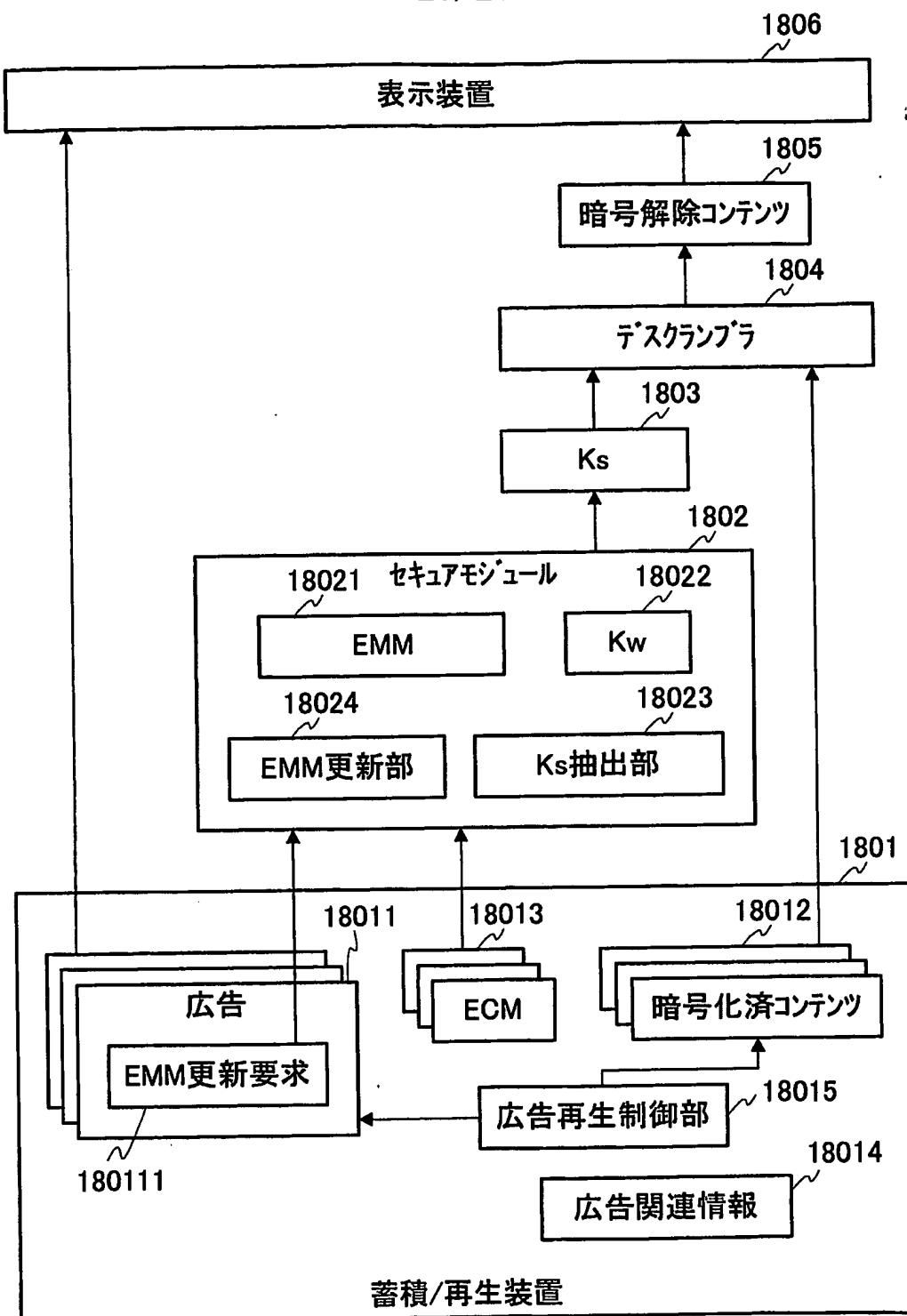


図27

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.